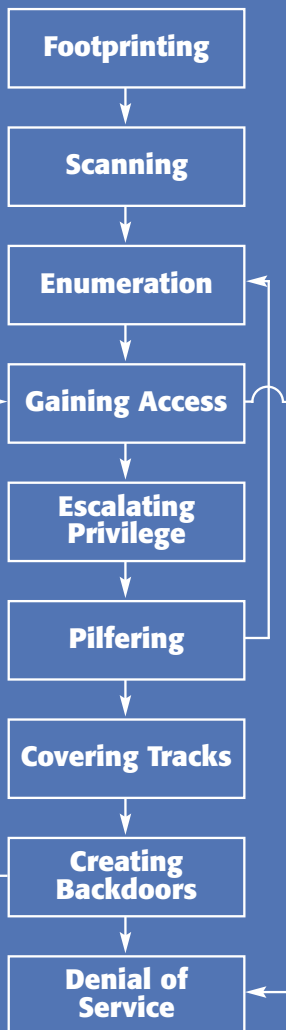


Harga NeoTek + CD:  
**Rp29.500,-** (P. Jawa)  
**Rp29.500,-** (Luar P. Jawa)  
**NEOTEK**  
 Dunia Teknologi Baru

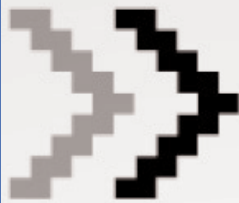
## Anatomi suatu serangan hacking



Lengkapi pengetahuan hacking dan PC security anda dengan berlangganan majalah NeoTek:

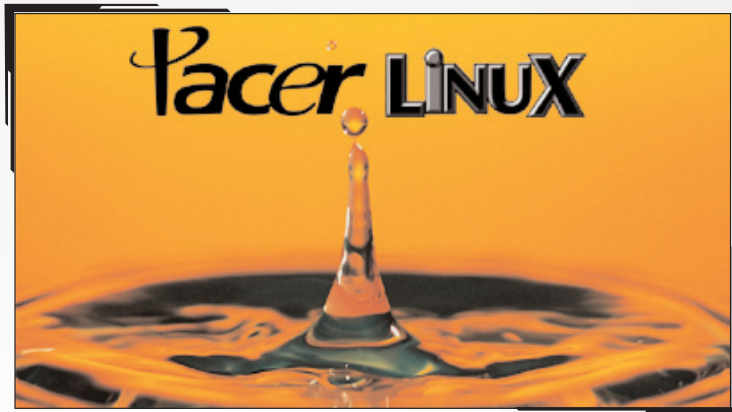
Hubungi  
**Aswan Bakri**  
 Tel. (021) 5481 457  
 HP. (0812) 9572043 (Aswan)  
 Email:  
 aswan\_bakri2001@yahoo.com  
 Kontak: Aswan Bakri

HomePage



# Salam!

## Open Source Movement 2006



• Bunyi gong Open Source masih terus bergema, Open Source Movement 2006 hadir menawarkan PacerLinux untuk seluruh pengguna komputer.

**G**aung akan Open Source ternyata belum surut, terbukti APKOMINDO yang didukung oleh PAZIA telah meluncurkan distro Linux yang diberi nama PACERLINUX yang merupakan singkatan dari Pazia Acer Linux. PACERLINUX yang di-bundle dalam produk ACER, diharapkan dapat menggantikan posisi LINPUS yang terlalu sederhana dan cukup sulit dimengerti oleh pengguna komputer awam.

Redaksi  
[redaksi@neotek.co.id](mailto:redaksi@neotek.co.id)

## Bagaimana menghubungi NEOTEK?

**KONTRIBUSI ARTIKEL**  
[redaksi@neotek.co.id](mailto:redaksi@neotek.co.id)

**SURAT PEMBACA**  
[support@neotek.co.id](mailto:support@neotek.co.id)

**WEBMASTER**  
[webmaster@neotek.co.id](mailto:webmaster@neotek.co.id)

**PEMASARAN**  
 Hedhi Sabaruddin, 0812-1891827

**CHATROOM DI DALNET**  
 #neoteker

**MILIS PARA NEOTEKER**  
<http://groups.yahoo.com/group/majalahneotek>

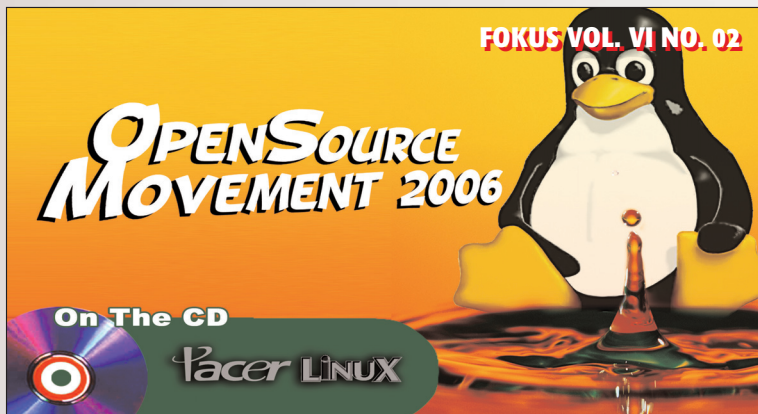
**ADMINISTRASI IKLAN**  
 Tel. 021-5481457 Fax. 021-5329041

**SIRKULASI NEOTEK**  
 Tel. 021-5481457

**ALAMAT REDAKSI**  
 4 Cairnhill Rise  
 #05-01 The Cairnhill  
 Singapore 229740  
 Telp. +65-67386482  
 email: kosasih@indo.net.id

# Daftar Isi

## NeoTek Vol. VI No. 02



### NeoRubrik

#### 9 Sudahkah Anda Aware dengan Web Sekuriti?

Kesadaran dan kepedulian terhadap keamanan adalah hal yang tidak dapat dilupakan begitu saja. Apakah anda sudah merasa cukup peduli dan sadar akan keamanan? Security Awareness adalah solusi jitu menciptakan keamanan.

### NeoStart

#### 10 From Fun to Profit

Hacking, berawal dari sebuah kesenangan pada akhirnya menjadi lahan nafkah.

#### 12 Bellua Cyber Security Asia 2006

Bellua Asia Pasific meluncurkan event Bellua Cyber Security 2006.

### Situs NeoTek

[www.neotek.co.id](http://www.neotek.co.id)

Jadikan situs NeoTek sebagai pangkalan Anda berselancar

#### Berlangganan

Formulir berlangganan (Hemat plus Bebas Ongkos Kirim) dapat di download di situs NeoTek.

#### NeoTek versi PDF

Kehabisan NeoTek di kota Anda? Dapatkan saja versi PDF-nya.

#### Quartely

Kini NeoTek terbit 4 kali setahun, dimulai dari edisi volume VI.

#### Layanan Rupa-rupa NeoTek

##### NeoTek Site

<http://www.neotek.co.id>  
Download PDF edisi lama.

##### NeoTek Mailing List

<http://groups.yahoo.com/group/majalahneotek>

##### Channel NeoTeker di Dalnet

Ngobrol ramai-ramai sesama NeoTeker di #neoteker server dalnet

##### NeoTeker Official Portal

Forum Neoteker  
<http://www.neoteker.or.id>

### NeoTutor

#### 14 PacerLinux Menjalankan Live-CD

Mengoperasikan PacerLinux untuk pertama kalinya sebagai Live-CD.

#### 15 PacerLinux Instalasi (Single Boot)

Teknik instalasi PacerLinux ke dalam Harddisk sebagai OS tunggal.

#### 18 PacerLinux Instalasi (Dual Boot)

Teknik instalasi PacerLinux ke dalam Harddisk yang terdapat MS Windows.

#### 21 PacerLinux Aplikasi Pendukung

Menjelajah software-software yang terdapat dalam PacerLinux.

#### 23 PacerLinux Network & Printer

Teknik melakukan setting jaringan dan Printer di PacerLinux.

#### 27 PacerLinux Samba Network

Dengan fasilitas Samba Network Neighbourhood membuat file sharing.

#### 28 PacerLinux KPackage

Membuang dan menambahkan software maupun driver di PacerLinux.

### NeoTekno

#### 30 E-Banking Tidak Hanya Internet

Apa itu E-Banking? Apakah hanya Banking Internet? Temukan jawabannya di edisi kali ini.

**32 E-Banking  
Produk dan Jasa**

Mengenal produk-produk dan jasa yang berkaitan dengan E-Banking.

**36 E-Banking  
Seluk Beluk Paypal**

Memahami Paypal sebagai salah satu alat pembayaran online.

**38 E-Banking  
E-Gold Lebih Jauh**

Memahami E-Gold sebagai salah satu alat pembayaran online.

**40 E-Banking  
Sisi Gelap**

Mengenal sisi negatif yang mengintai E-Banking.

**NeoRagam****4**

**Klak Klik**  
Tips Bulan Ini  
Nero ImageDrive

Panhac  
Roadshow Kompetisi  
Hacking di 9 Kota

**5**

Panhac  
Catatan Perjalanan  
PANHAC 2006

**44**

**Daftar Isi CD NeoTek**  
PacerLinux (Pazia Acer Linux)  
mengisi CD NeoTek.  
Distro baru yang akan  
menggantikan LINPUS

**NeoStyle****45 Adobe Photoshop  
Colour Focusing**

Hal yang paling mengasyikkan ketika berhadapan dengan Photoshop adalah melakukan editing, edisi kali ini akan memberikan trik membuat kesan fokus pada photo dengan teknik Color Mask.

**47 Easy Mosaic  
Photo Mosaic**

Easy Mosaic mewujudkan keinginan anda untuk menjadikan photo koleksi menjadi sebuah photo mosaic.

**NeoTek Vol. VI-No. 03  
Ancaman XSS Attack**

XSS (Cross-site Scripting) Attack memang bukanlah teknik yang dapat membahayakan sebuah server, tetapi tetap saja XSS Attack tidak dapat dipandang remeh karena dampak dari teknik ini terletak pada TRUST.

Trust? Kepercayaan pelanggan menjadi penting bagi usaha yang menyediakan jasa apa saja di Internet. Untuk itu penting untuk menjaga kepercayaan pelanggan.

Jika teknik XSS Attack dikombinasikan dengan teknik-teknik hacking lainnya. Hm..., what do you think?

**Perwakilan NeoTek**

Perwakilan NeoTek kini ada di daerah-daerah berikut:

**Candi Gebang Permai**

Candi Gebang Permai R-6  
Yogyakarta 55511  
Telp. 0274-882262/462135  
Fax. 0274-4462136

**Pamulang Permai**

Pamulang Permai Blok A No. 30  
Pamulang Barat Ciputat  
Jakarta Selatan 15417  
Telp./Fax. 021-7430589

**Griya Bukit Mas**

Griya Bukit Mas II D1/13  
Bojong Koneng Cikutra  
Bandung 40191  
Telp./Fax. 022-7218548

**Taman Pondok Indah**

Taman Pondok Indah Blok M/17  
Jl. Wiyung Indah Gg. IX  
Surabaya 60288  
Telp./Fax. 031-7660508

**Tulus Harapan**

Perumahan Tulus Harapan  
Blok B 13B No. 10  
Sedangmulyo, Tembalang  
Semarang

**Berlangganan**

Bagi Anda yang bedomisili di daerah perwakilan NeoTek, kini dapat langsung membeli atau berlangganan.

**Neolnbox****8**

**Diskusi sesama  
Neoteker di Milis  
NeoTek**

**NeoProfil****3**

**Editorial Office**

4 Cairnhill Rise  
#05-01 The Cairnhill  
Singapore 229740  
Telp. +65-67386482

**Business Office**

Gedung Cahaya Palmerah 503  
Jl. Palmerah Utara III No. 9  
Jakarta 11480  
Telp. 021-5481457  
Fax. 021-5329041

**Pemimpin Umum**

Fachri Said

**Pemimpin Redaksi**

Kosasih Iskandarsjah

**Redaktur Ahli**

Onno W. Purbo  
Michael S. Sunggiardi

**Pemimpin Usaha**

Fahmi Oemar  
Dadang Krisdayadi

**Redaktur Pelaksana**

MA Rody Candra

**Sekretaris Redaksi**

Marni

**Dewan Redaksi**

Dani Firman Syah

**Sirkulasi**

Hedhi Sabaruddin

**Adm. Langganan**

KRISHNAdISTRIBUTOR

**Iklan dan Promosi**

Gianto Widiyanto

**Keuangan**

Aswan Bakri

**Bank**

**Bank BNI**

a.n. PT NeoTek Maju Mandiri  
No. Rekening 0018301033

**Bank Central Asia**

(khusus untuk langganan)

Aswan Bakri

No. rekening 0940544131



## Klak Klik

TIPS BULAN INI  
Nero Virtual CD

**A**nda yang senang bermain PC game tentu pernah menemui kejadian CD game harus berada pada tempatnya di CDROM, jika tidak ditempatkan maka PC game tidak dapat dimainkan.

Jika CD PC game yang ingin anda mainkan adalah milik sendiri tentu bukan menjadi masalah. Permasalahan hadir jika anda bukan pemilik CD PC game tersebut.

Melakukan kopi CD bisa saja sebagai penyelesaian masalah, tetapi ada sebagian orang yang tidak menginginkan penggunaan CD ketika bermain game. Untuk itu masalah diselesaikan dengan menggunakan program Virtual CD.

Pembahasan mengenai program virtual CD pernah menghiasi halaman majalah ini.

Penggunaan program sejenis virtual CD pun masih dianggap terlalu menyusahkan, banyak orang yang tidak menginginkan penggunaan virtual CD.

Banyak orang yang tidak menyadari jika Nero yang dikenal sebagai program burning CD/DVD ternyata memiliki fitur yang sama fungsinya dengan program virtual CD. Fitur tersebut disebut ImageDrive.

Yang perlu anda lakukan adalah membuat file image versi Nero yaitu \*.nrg dari sebuah CD. Setelah proses pembuatan image selesai, aktifkan fitur imagedrive.

pada pertama kali fitur ini diaktifkan, permintaan restart akan anda temukan, lakukan restart. Setelah komputer kembali aktif, pada file image yang dibuat lakukan klik kanan dan pilih opsi open image drive.

## PANHAC - Roadshow Kompetisi Hacking di 9 Kota

**I**ni merupakan laporan mengenai roadshow kompetisi hacking, yang diberi nama **Pazia Acer National Hacking Competition 2006**, yang diselenggarakan di 9 kota besar di Indonesia.

**PT Acer Indonesia** bersama **PT Pazia Pillar Mercycor** mulai tanggal 18 Februari hingga 14 Maret menyelenggarakan kompetisi hacking nasional, **Pazia Acer National Hacking Competition (PANHAC) 2006**, yang di adakan di 9 kota besar di Indonesia. Acara ini merupakan pertama yang terbesar di Indonesia dan di dunia dengan dukungan 100 notebook yang dibawa ke 9 kota besar di Indonesia, yaitu: **Semarang, Jogjakarta, Medan, Padang, Bandung, Surabaya, Denpasar, Makasar dan Jakarta.**

Kompetisi hacking atau lebih di kenal dengan **Capture The Flag (CTF)**, merupakan event yang bersifat games dan edukasi di bidang teknologi keamanan jaringan komputer, yang mana di luar negeri event seperti ini sudah sering di adakan seperti di kampus-kampus dan di acara-acara konferensi teknologi. Kompetisi Hacking atau CTF merupakan lomba mencari dan menemukan celah keamanan di sebuah jaringan komputer yang sudah di buat berlubang oleh penyelenggara. Jaringan komputer ini di buat dan di simulasikan seperti layaknya jaringan Internet sehingga peserta lomba akan di tantang untuk mempelajari jaringan komputer panitia dan mencari celah yang sudah di buat oleh panitia.

Dalam acara PANHAC 2006 ini peserta diyakini tidak akan mengalami kesulitan dalam mencari atau menemukan lubang sekuriti yang sudah di rancang oleh panitia, karena hanya dengan menggunakan beberapa program scanning dan program sekuriti lain yang sudah tersedia di

Internet, peserta sudah mampu menganalisa jaringan komputer yang di desain panitia. Teknik-teknik yang bisa di gunakan oleh peserta juga relatif masih mudah, seperti scanning yaitu teknik mencari komputer yang aktif dan tersambung di jaringan, kemudian mencari kelemahan di salah satu komputer yang sudah disediakan oleh panitia.

Acara ini pada dasarnya lebih di tujukan untuk **fun and games**, disamping memberi kesempatan kepada peserta untuk saling bertukar pengetahuan dan teknologi keamanan jaringan komputer dengan peserta lain. Pada kompetisi ini, ada kemungkinan tidak ada yang berhasil menemukan lubang sekuriti yang sudah di rancang oleh panitia, tetapi semua peserta tetap akan mendapatkan point atau nilai sesuai dengan kriteria penilaian yang sudah di tentukan, dan bagi yang memiliki nilai tertinggi berhak untuk mendapatkan notebook **Acer Aspire 3620** sebagai hadiah di setiap kota dan **Acer Aspire 5670** sebagai hadiah utama.

Secara umum, peminat di setiap kota sebenarnya cukup besar, sayangnya, acara yang baru pertama kali diselenggarakan ini, ditanggapi dengan intip-intip saja oleh para jagoan dan komunitas **bawah tanah** (Under Ground). Ada juga yang takut membuka diri dan data sebagai hacker, selain yang ragu-ragu karena kata hacking dianggap sulit dan negatif.

Atas dasar itu, tahap pencarian peserta terasa sangat lambat dan sulit. Saat tim CEO mendatangi secara proaktif ke kampus-kampus, berinteraksi langsung dengan para calon peserta, ketertarikan terhadap acara mulai mening-

kat. Sebagian dari mereka mengaku tidak mengetahui acara ini, sebagian lagi sudah tahu tapi kurang mengerti dengan informasi yang disampaikan melalui flyer dan poster PANHAC.

Tanggapan peserta setelah mengikuti pertandingan, cukup positif. Banyak permintaan agar acara ini diselenggarakan per tahun disertai workshop dan seminar di awal kompetisinya.

Peserta PANHAC 2006 terdiri dari kalangan pelajar, mahasiswa, praktisi TI. Beberapa peserta menunjukkan minat belajar yang tinggi, disamping penasaran merebut gelar juara tentunya.

Panitia menantang semua peserta yang belum juara, untuk ikut di kota selanjutnya. Sehingga ada yang mengejar kompetisi di Medan dan Padang, di Semarang dan Yogya, bahkan Medan dan Bandung. Beberapa juara tangguh ada yang akhirnya jadi juara, tapi banyak yang tetap tidak berhasil, karena panitia punya seribu satu macam soal yang berubah-ubah di setiap kota.

Ajukan jempol untuk panitia disampaikan oleh peserta yang ikut di lebih dari satu kota. Hanya pemenang di Denpasar yang berhasil menembus target dan mendapat polongan logo PANHAC.

Akan lebih menarik lagi jika anda menyimak catatan perjalanan selama Roadshow PANHAC 2006 yang penuh suka dan duka yang ditemui CEO dan panitia pelaksana acara.





## PANHAC - Catatan Perjalanan PANHAC 2006

**S**imak catatan perjalanan PANHAC 2006 yang sukses diadakan di 9 kota besar di Indonesia.

### Perjalanan Dimulai Dari Semarang

Diikuti oleh 78 peserta yang terdiri dari perorangan dan 8 tim, yang terdiri antara dua dan tiga peserta. Jumlah peserta ini dibawah target 200 orang, karena kebanyakan calon peserta merasa khawatir mengikuti acara ini, bahkan beberapa orang tidak mengetahui apa yang disebut hacking. **Hacking ke gunung mana, mas? Hujan-hujan gini,** ketika ditawarkan untuk ikut acara ini.

Panitia PANHAC 2006 bersama sponsor acara ini, Pazia dan Acer menyepakati, bahwa dalam kompetisi nasional hacking ini, **pasti ada juara** di setiap kota, walaupun pada kenyataan tidak ada yang mampu mengambil file yang sudah disediakan oleh panitia.



Kesulitan dalam acara ini ternyata bukan bagaimana peserta bisa masuk ke server atau jaringan, tetapi teknologi yang dipakai oleh panitia, yaitu teknologi wireless LAN yang ada di setiap notebook peserta. Lebih dari 30 menit peserta berkuat mengaktifkan wireless LAN-nya, dibantu oleh asisten dari Universitas AKI, karena kebanyakan peserta belum pernah menggunakan teknologi wireless LAN yang disediakan oleh panitia.

Akhirnya nilai tertinggi diberikan kepada tim **NOTHING TO LOOSE** dengan kriteria berhasil melakukan scanning terlama ke jaringan server. Mereka terdiri dari **Prabowo Bayuaji, Franky Yustanto**, serta **Lucky Widianto**.

### Semakin Seru di Kota Gudeg Jogjakarta

Jogjakarta sebagai kota pelajar dan memiliki banyak anak muda berbakat dalam bidang komputer, ditantang oleh tim PANHAC untuk **membobol** server yang telah dirancang oleh panitia. Kompetisi yang bertempat di Universitas **Kristen Duta Wacana**,

panitia dibantu beberapa rekan mahasiswa dari Universitas setempat saling berkerjasama dan bekerja keras agar peserta maupun panitia dapat merasakan keamanan serta kenyamanan pada saat kompetisi berlangsung.

Kompetisi diikuti 104 peserta dimulai pada pukul 09.00 WIB, di Universitas Kristen Duta Wacana. Mengacu pada pengalaman di Semarang, dimana sebagian besar peserta belum mengerti bagaimana menyambung komputer-nya dengan jaringan wireless yang ada di sekitar ruangan, panitia memutuskan untuk memberikan penjelasan singkat mengenai cara-cara menyambung notebook yang mereka pakai ke **Access Point** yang sudah disiapkan panitia.



Acara berlangsung menarik yang membuat panitia tersenyum karena banyak peserta yang merasa akan berhasil menembus server target. Untuk 20 menit pertama, banyak peserta yang masuk ke server bayangan yang disiapkan panitia, tetapi semuanya pada network yang berbeda dengan server target.

Panitia berusaha memberikan sedikit petunjuk dengan memperlihatkan log trafik dari jaringan dimana server target berada, sampai pada nama **Access Point** yang menjadi pintu gerbang jaringan server aslinya.

Waktu serasa melaju sangat cepat, peserta harus segera mengakhiri perburuannya dan segera mengisi lembaran yang ada di meja, karena isian tersebut merupakan salah satu faktor penilaian dari dewan juri.

Lebih kurang 20 menit dewan juri yang terdiri dari perwakilan dari **Pazia, Rusmanto, Michael S. Sunggiardi** dan **Dani Firman Syah** berunding untuk menentukan sang juara.

Akhirnya dewan juri memutuskan tim **NEWBEEZ** sebagai pemenang untuk Jogjakarta. Tim **NEWBEEZ** yang terdiri dari **Andreas Kisworo** dan **Dafi Hirdhananda**, mahasiswa Universitas Kristen Duta Wacana yang

memang tertarik pada dunia IT terutama keamanan jaringan komputer.

Menurut sumber yang dapat dipercaya, anggota tim **NEWBEEZ** adalah asisten dosen dan sering mengikuti perlombaan sejenis. Pada kompetisi kali ini belum bisa mendapatkan file yang dicari karena waktu pertandingan yang terlalu singkat serta diserangnya notebook tim **NEWBEEZ** oleh banyak peserta lain yang mempersulit tim **NEWBEEZ** sendiri untuk mencari informasi lebih jauh mengenai server target.

### Medan yang Menantang

24 Februari 2006, Medan sebagai kota ke tiga dari acara roadshow, berlangsung di **Universitas Mikroskil Medan**. Jumlah peserta yang mendaftar untuk **Medan** ini sekitar 89 orang.



Server target yang digunakan masih sama dengan dua kota sebelumnya dan **Access Point** yang digunakan masih dengan jumlah yang sama, hanya kali ini untuk **essid**, tim PANHAC memilih nama-nama warna yaitu merah, putih, gold, silver, coklat, kuning, hijau, biru, orange, dan pink.

**Pink** merupakan **Access Point gateway** menuju server target, tanpa enkripsi apapun seperti WEP dari teknologi WLAN. Satu jam berlalu, belum ada yang bisa mendapatkan file di target server, walaupun beberapa peserta sudah ada yang berhasil mengidentifikasi server maupun memasuki jaringan yang sama dengan server target.

Terjadi persaingan nilai antara peserta, sehingga khusus di Medan ada dua juara, yaitu tim **DES** dan tim **PAJUS**. Tim **DES** memenangkan hadiah utama berupa notebook **Acer Aspire 3620**, sedang tim **PAJUS** mendapatkan sebuah switch 5 port dari **LevelONE**. Lebih khusus lagi, kedua tim berhak untuk ikut di grand final di Jakarta.

Tim **DES** terdiri dari **Desdulianto** dan **Rudy**, keduanya akan berusaha agar di Jakarta nanti bisa mendapatkan

## NeoRagam

hadiah utama yaitu notebook Acer Aspire seri 5670. Selamat untuk tim DES.

Tim PAJUS terdiri dari **Andri Wardhana, Imam dan Rudy Malvin** menyampaikan rasa penasaran mereka karena tidak berhasil mendapatkan juara pertama. Mereka bertekad akan ikut lagi di kota selanjutnya, Padang.

### Padang Nan Rancak Bana

Tiba di Bandara Minangkabau Sabtu sore. Bukit barisan menyambut dengan ramah, setelah sehari sebelumnya diguyur hujan cukup deras dan berkepanjangan.

PANHAC 2006 diselenggarakan di Universitas Negeri Padang pada tanggal 28 Februari 2006. Acara dibuka dengan sambutan rektor dan dekan UNP yang menyampaikan tanggapan positif atas terselenggaranya acara ini. Harapan semua, bahwa para hacker akan memanfaatkan keahlian mereka untuk kemajuan bangsa.

Kali ini, panitia merubah OS server menjadi Linux, karena sudah kelihatan banyaknya peserta yang ikut untuk kedua kalinya. Pertandingan di antara 151 peserta berlangsung seru, dan dalam waktu singkat, banyak peserta yang berhasil masuk jaringan.



Padang membuktikan kehebatan komunitasnya. Muncul dua orang pemenang perorangan di kota ini, dengan NILAI SAMA! Akhirnya, untuk mencegah kejadian di Medan, dimana ada dua pemenang, panitia PANHAC 2006 memutuskan untuk menyelenggarakan pertandingan ulang dalam penambahan waktu.

Walaupun belum ada yang berhasil mengambil file dari server target, **Deddy Syefria** dari UNP berhasil menyabet notebook Acer 3620 dan diundang ke Jakarta. Sedangkan **Syukhri** harus puas dengan switch 5 port dari LevelONE.

### Kejutan di Kota Factory Outlet - Bandung

Kejutan apa? Ada pelajar 4 SMP asal Bontang dan Banjaran. Lebih heboh lagi, seorang siswa SD berusia 11 tahun - **Aiman Alauddin Fadrullah Al-**

**fath** ikut kompetisi! Dia memang tidak sendiri. Satu tim dengan ayahnya yang dikenal sebagai pemain lama di dunia internet, seorang dosen TI dari ITB, mereka sangat menarik perhatian di antara 112 orang peserta yang bertanding hari itu di Universitas Kristen Maranatha, 02 Maret 2006.

Selain peserta termuda, di Bandung banyak juga peserta dari komunitas bawah tanah yang mulai keluar, satu diantaranya sakit jiwa yang punya nama besar di dunia hacker Indonesia. Ada juga 3 orang yang tidak ingin diketahui identitasnya bergabung dalam satu tim.

SPG cantik sexy tapi tidak tepat waktu, menyegarkan suasana kompetisi yang didominasi warna hitam dan pejection.



Pergulatan yang seru menyerbu server, saling sikut antar peserta, akhirnya harus berakhir setelah 60 menit berlalu. **Aristo S. Hadi Soeganda, Yoseph Ronald Soetanto, Ignatius Reza Lesmana** dari UNPAR berhasil merebut notebook Acer Aspire dari komunitas bawah tanah. **Fery Usamah** di tempat kedua memperoleh switch dari LevelONE.

### PANHAC Sambil Tepuk Nyamuk di Surabaya

Berbeda dengan kota lain, kompetisi di Surabaya dan Makassar berlangsung di pusat pertokoan. Di Surabaya diselenggarakan di Hi-Tech Mall atau yang lebih dikenal dengan area THR-Taman Hiburan Rakyat, dimana tempat ini menjadi saksi para hacker Surabaya beraksi.

Panitia lembur sampai tengah malam untuk mempersiapkan peralatan lomba. Untunglah tim panitia telah terbiasa dengan kehidupan malam sehingga pagi hari sudah siap menyambut para peserta.

Acara dibuka dengan sambutan dari Pazia, kemudian dilanjutkan penjelasan acara dan pengenalan teknologi W-LAN. Arena lomba terasa sangat padat dengan 95 orang peserta. Lebih khas lagi, ternyata di sini tim PANHAC 2006 ditemani nyamuk-nyamuk yang mengamuk. Mungkin ingin dapat kaos tapi tidak ada yang pas. Ma-

ka panitia dan peserta sibuk tepak-tepuk di sekitar kaki dan telinga.



Pertandingan berlangsung cukup seru terutama dengan keikutsertaan peserta penasaran dari Jogjakarta. Akhirnya, peserta dari Jogja ini yang menjadi pemenang. **Aizza Jundana** meraih juara pertama, pasangan **Krisna dan Kosha** di tempat kedua. Padahal, pasangan ini hampir masuk server dan meraih juara pertama, tapi sayang notebook tiba-tiba off karena kabel power tidak tersambung. *Kami akan datang ke Denpasar!*, tekad Krisna dan Kosha.

### Denpasar Meraih Logo PANHAC

Berangkat dari bandara Juanda Surabaya pukul 12.00 WIB, tiba di bandara Ngurah Rai pukul 14.50 WITA. Dalam waktu sekejap, kami sudah berada di wilayah waktu yang satu jam lebih cepat. Setelah check in di Harris Hotel yang bernuansa minimalis modern, tim PANHAC berangkat ke Universitas Udayana.

Tidak terbayang sebelumnya, ternyata panitia harus mengangkut 550 kg barang ke lantai empat gedung kampus Pasca Sarjana Unud - tanpa lift! Dengan bantuan tim Balisoft sebagai partner lokal, akhirnya barang diangkut dan proses instalasi berjalan lancar.



**Krisna dan Kosha** membuktikan tekad mereka. Vini vidi vici. Mereka datang untuk berhasil. Tidak tanggung-tanggung, 4 potongan logo PANHAC berhasil diperoleh! Pejuang tangguh ini meraih juara satu dan akan hadir di grand final Jakarta. Sedangkan pasangan **Michael Jimmy, M. Hasran Addahroni** meraih juara dua.



### Hacker Kota Ayam Jantan dari Timur

Belajar dari pengalaman. Itulah kalimat yang tepat untuk panitia PANHAC. Dari kota ke kota selalu menyesuaikan dengan pengalaman sebelumnya. Mengingat banyak peserta yang meminta ada seminar sebelum workshop, di Makassar, kompetisi di mulai dengan presentasi tentang security selama 30 menit.

Setelah disusul dengan pembukaan dari **Yenny**, wakil Pazia, penjelasan-penjelasan lomba, maka 139 peserta mulai beraksi di MTC Karebosi Lt 5 pk 14.10 WITA. Tentu level kesulitan dan detail teknis berubah di tiap kota. Sehingga, peserta penasaran dari Denpasar – **Michael Jimmy** terpaksa mengaku kalah dari jagoan Kota Ayam Jantan dari Timur.



**Ahmad Attas**, juara pertama yang berhasil memperoleh 2 potongan logo PANHAC, dan **Fadli Ayub** juara kedua berhasil memperoleh 1 potongan logo.

Ketika ditanya panitia, **Mimpi apa semalam Bang Ahmad?** Jawabnya, **Dapat menara tinggi.** Mungkin itu pertanda keberuntungan ini.

### Kamp Darurat di Mega Bazaar JHCC

10 Maret 2006, *landing* di Soekarno Hatta langsung meluncur ke Mega Bazaar Balai Sidang untuk setting acara selanjutnya. Sesuai instruksi, Kami langsung mengatur turun bongkar barang, mencari ruang workshop di *connecting area*. Loh koq tidak ada?! Kata panitia Dyandra, ruangan PANHAC bukan di sana. Diajaklah kami menuju sebuah pintu yang tadinya tidak tampak, terletak di belakang salah satu booth pameran.

Terkejut ketika melihat setting ruang mirip warnet dengan sekat tertutup, berkapasitas 60 meja. Design tidak dapat dirubah, menyulitkan untuk pengaturan tempat tas peserta, dus-dus barang, registrasi. Ruangan yang mirip kamp darurat ini kurang layak untuk acara ini.

Berhimpit-himpit 87 peserta mengelilingi meja registrasi untuk mendapatkan nomor kursi dan kaos PANHAC. Tampak peserta gentayangan dari Bandung, Bali, Semarang dan Makassar turut hadir. Kejutan saingan peserta Bandung, di sini hadir peserta peorangan usia 12 tahun dari Sekolah Kesatuan Bogor, **Mickeel Pramono**.



**Wahyu Fitri Riyanto** berhasil membawa pulang hadiah notebook Acer Aspire 3620. Pasangan kekasih **Ahmad Maulana & Farisah Amanda** yang daftar terlambat 15 menit boleh berbangga meraih juara dua dan mendapatkan Switch LevelONE.

### Audisi yang meriah di JACC Mangga Dua Mall

Kali ini, setting ruangan hall lantai dasar Jakarta Computer Center Mangga Dua Mall. Pagi 14 Maret, 08.00. Panitia bergegas melakukan persiapan kompetisi. Walaupun sempat kepepet karena kantor JACC tempat penitipan barang-barang baru dibuka jam 10.00, pertandingan 107 peserta terselenggara dengan lancar dan meriah.

Di antara peserta, tampak peserta bule yang sudah menikah dengan WNI dan berdomisili di Jakarta ikut berpartisipasi. Lebih kurang 20 menit kompetisi berlangsung, panitia mensinyalir adanya sabotase terhadap kompetisi. Selama beberapa saat, hampir seluruh peserta kesulitan mengakses jaringan.



Dikatakan oleh panitia, *Hentikan tindakan pengrusakan atau sabotase jaringan. Jika dilakukan*

*oleh peserta, akan didiskualifikasi. Jika dilakukan oleh pihak luar, akan ditindak tegas!*

Tidak disangka, bule bernama **Luis Perez** jadi juara pertama.

### Piagam MURI untuk Acer dan Pazia

Menjelang acara Grand Final, Bapak **Okke**, wakil MURI – Museum Rekor Indonesia menyampaikan piagam penghargaan kepada Acer sebagai pembuat rekor kompetisi Hacking pertama di Indonesia dengan menggunakan Notebook Acer Aspire. Piagam kedua diserahkan kepada Pazia sebagai pemrakarsa acara. Semoga bermanfaat bagi nusa dan bangsa, pesannya.



### Ayam Jantan dari Timur - Sang Juara Sejati

Misinya kali ini adalah menemukan logo PANHAC, mendapatkan file foto dari peserta lain, dan mempertahankan file foto yang terdapat di dalam notebook-nya. Ada 20 file gambar berkelieran di jaringan untuk menentukan penilaian.

Satu jam yang menegangkan dimulai, para penonton turut asyik karena diperbolehkan melihat kegiatan saling hack di monitor panitia.



Juara pertama: **Ahmad Attas** dari Makassar

Juara kedua: **Prabowo Bayuaji, Franky Yustanto, Lucky Widiyanto** dari Semarang

Juara ketiga: **I Gede Putu Krisna J, I Gede Bagus Kosha P**, dari Bali





# NmN

## Neoteker menjawab Neoteker

Forum ini dimaksudkan sebagai bentuk *offline* dari *mailing list* NeoTek di <http://groups.yahoo.com/group/majalahneotek>.

### T: Posted May 4

Saya mencari pigtail dengan konektor RP-SMA, untuk di pasan ke WLAN card SMC 2802W. bagi rekan-rekan yang menjual pigtail yang support dgn card saya tersebut bisa kirim gambar + spesifikasi ke yusda\_46@yahoo.com pigtail buatan sendiri pun tidak masalah, yang penting ada garansi dan menggunakan konektor RP-SMA.

yusda  
yusdas@yahoo.com

### J: Posted May 4

Hello yusda, my answer is klo anda di bandung bisa maen ke [www.cigadung.com](http://www.cigadung.com) klo beli konektornya doang harganya kira2 70 ribu-an. Nero Sumargono  
itpribadi@yahoo.com.sg

### J: Posted May 5

Mas bikin aja sendiri, posisi dimana kalo di jakarta ke kenari aja di jalan kenari 1 toko sinar waja di situ jual macam2 alat buat antena dan kalo kita mau bikin pigtail juga bisa

Rgds

Yanriz  
yanriz@centrin.net.id

### J: Posted May 5

pigtail di Sinar Waja mahal lebih baik ke Glodok lantai 1 lebih murah ada toko yang bisa bikin Rp. 50.000,-

Glodok Lantai 2 Breaker Shop bisa bikin juga agak mahal sih sekitar Rp. 70.000,-

Onno W. Purbo  
onno@indo.net.id

### T: Posted May 7

saya posisi di Malang, ada yang tau gak klo untuk daerah malang tempat yang menjual berbagai keperluan untuk bikin pigtail. saya sudah cari di toko-toko yang menjual alat-alat listrik tapi gak ada yang menjual konektor RP-SMA, kalo konektor N nya kan bisa aja diganti dengan RG-8. atau mungkin ada rekan yang bersedia bantu saya untuk bikin pigtail di tempat yang pak Onno W. Purbo sebutkan tadi, trus nanti bersedia mengirimkan ke alamat saya (08170534738). Seluruh biaya yang dikeluarkan akan saya ganti, dengan transfer bank....

Sebelum dan sesudahnya saya ucapkan terima kasih

yusda  
yusdas@yahoo.com

### J: Posted May 9

Mas kalo gak ke surabaya aja di pasar genteng...

Yanriz  
yanriz@centrin.net.id

### T: Posted May 5

Rekan-rekan,  
Bagaimana cara tes bandwidth koneksi internet yang sedang kita gunakan dari sebuah ISP? Apakah ada software khusus buat mengukur bandwidth speed? Misalnya kalau kita menggunakan koneksi ADSL 512 Kbps, apakah benar kita mendapatkan segitu? Soalnya saya berencana mengganti koneksi ADSL ke Wireless, tapi khawatir dibohongi ISP tentang besarnya bandwidth yang diterima, baik UP, DOWN dan koneksi internasional. Terima kasih atas

pencerahannya.

Salam,  
RedStorm  
RedStorm@indo.net.id

### J: Posted May 5

Ini sekedar pengalaman pribadi.

Test ke Link IIX  
(indonesia):

1. [www.sijiwae.net/speedtest](http://www.sijiwae.net/speedtest)
2. [www.indosatm2.com](http://www.indosatm2.com)

Internasional:

[www.speakeasy.net/speedtest](http://www.speakeasy.net/speedtest)

eko wahyu nugroho  
e\_wahyu@yahoo.com

### T: Posted May 10

Rekan milis YTH,  
Belakangan ini saya terfikir bagaimana cara 4444 (registrasi kartu pra bayar) membuat mesin penjawab SMS berbasis computer, untuk itu saya mohon bantuan rekan2 untuk menjelaskan hal2 berikut:

1. Bagaimana cara membangun interaksi antara computer & HP
2. Selain HP & Komputer adakah alat bantuan lain
3. Apakah bisa nomor pribadi dibuat seperti 4444

Terima kasih sebelumnya

Hendra Hermawan  
hendra.hermawan@suzuki.co.id

### J: Posted May 10

1. Anda membutuhkan sebuah modem di komputer dan kabel data HP (untuk hubungan komp dan HP). lalu diperlukan program/sistem informasi untuk menjawabnya. dimana setiap ada SMS masuk ke HP secara otomatis akan masuk kedalam komputer. kemudian program komputer memerintahkan untuk

membalas atau me-reply-nya.

kalo ingin coba gratis, cari pake google dengan kunci:  
- membuat sms server  
- make sms server

ato coba program seperti:  
- kannel  
- playsms  
- ozeki

2. Ya modem itu.

3. Kalo nomer pribadi ini, anda harus kontak ke telkom dahulu. kerja sama begitu. soalnya nomer-nomer ini masih dipegang oleh telkom dan belum sepenuhnya dipegang oleh menkominfo.

Mungkin begitu penjelasan saya. kiranya teman-teman bisa menambahkan ato mengkoreksi.

Terima kasih.

Agus Muhajir  
hajirodeon@yahoo.com

### J: Posted May 10

Saya mengembangkan aplikasi seperti ini namanya rakeyan SMS Management yang menggunakan GSM/CDMA modem (jadi sudah tidak menggunakan HP lagi sehubungan memory dan kecepatannya yang relatif lebih lambat. (Aplikasi ini sudah digunakan di Bandung oleh Gubernur dan Kapolda serta jajaran nya [www.jerbee.co.id](http://www.jerbee.co.id)).

Untuk interaksinya secara umum menggunakan AT Command, SMS yang masuk atau pengiriman SMS, agar mudah diatur secara periodik melakukan penyimpanan SMS yang masuk ke DB dan pengiriman SMS disimpan dulu ke DB baru ke alat.

Wahyudi  
wahyudi1@gmail.com

## SUDAHKAH ANDA AWARE DENGAN WEB SEKURITI?



**Security Awareness** (kesadaran/kepedulian terhadap keamanan), satu hal yang selalu dilupakan atau sengaja dilupakan oleh pihak-pihak yang menggunakan IT sebagai alat bantu kerja yang penting. Menyalahkan sosok Hacker adalah satu-satunya jalan untuk menutupi kesalahan. **Dani Firman Syah** (xnuxer@yahoo.com) memaparkan pentingnya Security Awareness untuk menghindari berbagai serangan yang dilakukan oleh oknum yang tidak bertanggung jawab..

**M**ASALAH KEPEDULIAN TERHADAP masalah web sekuriti merupakan **issue** yang menarik untuk diangkat kembali, setidaknya hal ini bisa digunakan sebagai bahan evaluasi supaya kita lebih berhati-hati dan lebih memperhatikan masalah web sekuriti. Bukan tanpa alasan kenapa masalah kepedulian terhadap web sekuriti dibahas dalam rubrik kali ini apalagi jika kita review kembali statistik yang dikeluarkan oleh **CSI** (Computer Security Institute)/**FBI** dan **Gatner Group** dalam laporannya di sebutkan:

- Data dari FBI/CSI tahun 2002, 95% insiden yang berkaitan dengan kasus hacking terjadi di web services.
- Bahkan Gatner Group melaporkan bahwa 70% serangan yang mengenai web terjadi di layer aplikasi web dan bukan di layer network.
- Data tahun 2001 saja insiden web aplikasi di beberapa perusahaan sudah mengakibatkan kerugian sebesar \$320 juta. Belum lagi hasil survey **Computer Institute** dan **FBI Computer Intrusion Squad** di tahun 2002 menunjukkan dari sekitar 223 responden (20% dari jumlah responden) melaporkan kerugian (financial loss) sebesar \$455 juta.

Dari data di atas jelas ada financial loss yang lumayan besar akibat adanya impact sekuriti di web dan tentunya ini memberikan kewaspadaan dan kepedulian kita

untuk membuka mata bahwa masalah web sekuriti seharusnya menjadi salah satu point penting yang paling tidak sudah direncanakan untuk diterapkan dalam **assessment** dan **penetration test** di perusahaan Anda. Apalagi jika proses bisnis di perusahaan Anda menggantungkan sepenuhnya pada data-data transaksi yang di transformasikan melalui aplikasi web.

Perkembangan selama setahun ini dilihat dari database **CVE** (Common Vulnerabilities and Exposures), lubang sekuriti yang terjadi di web aplikasi menduduki peringkat terbanyak dibandingkan lubang sekuriti diaplikasi network lainnya dan hal ini menurut analisa dari statistik **ZONE-H** terjadi dikarenakan oleh beberapa hal yang jika kita lihat dari data statistiknya memperlihatkan **mis-konfigurasi** dan **mis-programming** masih memberikan kontribusi yang terbesar terhadap timbulnya insiden sekuriti.

Kesalahan konfigurasi tentunya merupakan faktor **human-error** yang terjadi bukan karena kesengajaan tapi seringkali karena ketidaktahuan dari konfigurator yang melakukan **setup** dan **setting** di sistemnya. Sebuah aplikasi yang memiliki **hole** atau lubang sekuriti tentu juga bukan karena kesengajaan dari programmer untuk membuat aplikasi buatannya berlubang tapi lebih banyak terjadi karena ketidaktahuan programmer tentang cara membuat sebuah **code** program yang aman. Dengan melihat hal ini perlu bagi kita yang terjun di dunia teknologi informasi baik system administrator, programmer maupun user untuk lebih aware terhadap masalah-masalah sekuriti komputer dengan selalu mengupdate skill dan pengetahuannya dengan ilmu yang selalu di **update** dengan informasi sekuriti dan teknologi-teknologi baru.

### Statistik Zone-H.org

#### By attack method:

configuration / admin. mistake	17.7%	
known vulnerability (i.e. unpatched system)	13.9%	
undisclosed (new) vulnerability	12%	
File Inclusion	10.3%	
brute force attack	7.1%	
FTP Server intrusion	5.9%	
Not available	5.1%	
Attack against the administrator/user (password stealing/sniffing)	4.7%	
Other Web Application bug	4.4%	
SQL Injection	3.6%	
social engineering	3.3%	
Web Server intrusion	3.2%	
Access credentials through Man In the Middle attack	1.7%	
Other Server intrusion	1.3%	
Web Server external module intrusion	0.9%	
SSH Server intrusion	0.8%	
DNS attack through cache poisoning	0.7%	



# HACKING/CRACKING From Fun to Profit

**Bellua Asia Pasific** meluncurkan event akbar yaitu **Bellua Cyber Security Asia 2006**, berlangsung mulai dari tanggal 28 sampai 31 Agustus. Sebagai perkenalan, **Jim Geovedi** (jim@geovedi.com) pemerhati masalah keamanan komputer, memaparkan akan pentingnya nilai informasi dari sudut keamanan.

**D**UNIA INI TIDAK PERNAH ADA YANG BERSIFAT TETAP, segala sesuatu pasti berubah. Satu-satunya hal yang tetap adalah perubahan itu sendiri.

Perubahan terjadi umumnya karena ada sumber daya yang mulai terbatas atau penilaian terhadap sumber daya tersebut menjadi tinggi. Dalam majalah **Wired** edisi **Mei 2006**, terdapat iklan **General Motors Corporation** yang mengkampanyekan penggunaan bahan bakar **E85 ethanol**, sebuah bahan bakar alternatif yang dibuat dari 85% ethanol (yang dihasilkan dari jagung) dan 15% gasoline. Kesadaran akan mulai terbatasnya bahan bakar minyak menjadikan orang semakin inovatif dan hal tersebut seolah mengingatkan tentang bagaimana nilai dari sebuah informasi, dari sudut pandang keamanan, juga dapat berubah.

**Aleph One** (yang bernama asli Elias Levy dan juga adalah salah satu moderator mailing-list security Bugtraq), di dalam profilnya yang dimuat di majalah elektronik **Phrack, Issue 50** (April 1997), mengutarakan bahwa setiap sistem yang terhubung ke jaringan dapat dibobol. Hanya masalah waktu sebelum para hacker yang *iseng* menjadikan sistem tersebut sebagai target dengan menggunakan warez terbaru (kini dikenal sebagai **0-day**, tidak hanya untuk exploit atau tools namun juga untuk informasi vulnerability) untuk mem-bypass perlindungan firewall dan membobol sistem yang menjadi target.

Apa yang menjadi tujuan dominan dari para hacker *iseng* pada waktu itu adalah web page defacement atau menghancurkan sistem. Jika meninjau statistik dari situs Internet security termometer, **www.zone-h.org**, trend web page defacement masih dominan sampai hari ini terutama bagi para hacker pemula. Namun ternyata tidak untuk trend menghancurkan sistem karena para hacker sudah mulai mengetahui nilai dari sistem yang menjadi target berdasarkan fungsinya, sebagai contoh mesin yang berfungsi sebagai gateway, mail server atau hanya sekedar workstation biasa.

Tidak ada sistem yang tidak ada nilainya, sehingga salah besar jika seseorang masih menganggap komputer yang dimilikinya tidak bernilai. Penilaian dari sebuah sistem tidak hanya berpatokan pada hardware namun juga pada konten yang dimiliki seperti sistem operasi, aplikasi, maupun data yang disimpan.

## Bermotivasikan Uang

Seperti halnya jagung yang semula hanya dikenal sebagai bahan pangan, saat ini dapat diberdayakan menjadi bahan bakar alternatif. Hacking/cracking juga dapat diibaratkan telah mengalami perubahan dalam penilaian. Jika dahulu hacking/cracking cenderung hanya dikenal sebagai aktivitas pengisi waktu luang atau sekedar menyalurkan adrenalin (terutama ketika dalam menyusup sebuah sistem

remote), saat ini hacking/cracking lebih mengarah kepada aktivitas yang lebih profitable. Hacking/cracking yang dimaksud adalah aktivitas mencari kelemahan pada sebuah sistem dan mencari cara untuk mengeksploitasinya, menguasai sebuah sistem komputer dan menyewakannya sebagai spam relay atau menjadikannya agen distributed denial-of-service.

Dahulu para hacker/cracker mengutamakan ketenaran atau sekedar mengisi waktu luang dengan berbagai macam cara; mulai dari melakukan hal-hal yang baik seperti membangun sistem operasi atau aplikasi, sampai yang sebaliknya seperti membuat zombie networks, defacement web pages, menulis virus atau trojan, atau hal-hal yang cenderung merugikan orang lain. Saat ini, mereka nampaknya lebih termotivasi oleh uang.

Sehubungan dengan hal tersebut, ternyata ada banyak *pasar gelap* sebagai tempat bertransaksi antara hacker/cracker dengan pembeli. Seorang hacker yang menemukan cara mengeksploitasi cacat pada sistem Windows dapat memperoleh setidaknya US\$ 500 atau lebih, tergantung dari jumlah target yang terkena dampak atau nilai kritis yang diakibatkan, di pasar gelap tersebut. Akan lebih tinggi lagi nilainya jika cacat yang dimaksud merupakan *barang baru* (0-day vulnerability) dan belum pernah diketahui sebelumnya oleh Microsoft atau orang lain.

Cacat tersebut dapat dimanfaatkan untuk mengeksploitasi komputer. Komputer-komputer yang sudah dikuasai dapat dihubungkan menjadi satu dan dikontrol oleh sebuah master, dikenal sebagai botnet (dari kata robot network), dan kemudian dapat disewakan untuk digunakan sebagai spam relay, hosting untuk website porno, atau untuk mengirimkan serangan distributed denial-of-service.

## Rise of The Robots

0-day vulnerability ternyata juga dimanfaatkan untuk kepentingan segelintir orang dengan maksud yang tidak baik. Jika sebuah Internet worm dapat dibuat berdasarkan 0-day vulnerability, maka ancaman keamanan akan semakin meningkat. Seperti yang sudah disinggung di atas, bahwa ada pihak-pihak yang memang sengaja membuat worms dan kemudian berusaha menjadikan komputer-komputer yang sudah dikuasai untuk dapat dikontrol secara terpusat. Komputer-komputer zombie tersebut kemudian disewakan untuk aktivitas yang cenderung bersifat kriminal.

Botnet dapat melakukan hal-hal yang sifatnya merusak lebih dari sekedar mengirimkan spam dan phishing scams. Botnet seringkali menjadi agen distributed denial-of-service yang mengancam sebuah instansi berskala besar, melakukan Google dan Yahoo advertising click fraud, dan juga sebagai hosting dari phishing sites.

Software yang digunakan pada sebuah bot seringkali



dilengkapi dengan keylogger yang mampu merekam setiap input yang diberikan oleh pengguna, mencuri username dan password, informasi Internet banking, dan juga nomor kartu kredit.

Belum diketahui dengan jelas berapa banyak uang yang dapat diperoleh ketika seseorang menyewakan botnet-nya yang terdiri dari ratusan ribu hosts. Pernah ada kasus, dimana seseorang yang semula dikira hanya memiliki kurang lebih 100.000 komputer zombie ternyata memiliki lebih dari 1,5 juta komputer zombie.

Symantec melalui Internet Treat Report-nya menyebutkan bahwa kurang lebih 26% dari komputer yang termasuk kedalam botnet berlokasi di Amerika Serikat. Hal tersebut dimungkinkan karena penggunaan komputer rumah sudah semakin banyak dan kurangnya kewaspadaan pengguna tentang masalah keamanan komputer. Komputer-komputer yang memiliki aplikasi yang *bermasalah* setelah dikuasai kemudian dihubungkan untuk tujuan yang tidak baik.

### 0-Day Vulnerability Market

Sesuatu tersedia di pasar oleh karena ada yang membutuhkan, atau sebaliknya. Ketika sudah semakin banyak yang menyadari bahwa informasi vulnerability tidak lagi menjadi barang yang murah, maka banyak orang berlomba-lomba untuk mendapatkannya. Transaksi jual-beli informasi vulnerability dapat dilakukan dengan banyak cara. Mulai dari jenis transaksi primitif dimana pembeli dan penjual berhubungan secara langsung sampai dengan transaksi yang lebih moderen dimana pihak ketiga (broker) turut ambil andil.

Tidak banyak pemain dibidang usaha ini. Beberapa pemain yang tercatat antara lain **iDefense** dan **TippingPoint** (sebuah divisi dari 3com). Kedua perusahaan asal Amerika tersebut mempunyai program yang memungkinkan hacker dapat menyalurkan hasil temuan dan menukarkannya dengan dollar. Vulnerability Contribution Program dari iDefense sudah berlangsung setidaknya empat tahun sementara program Zero Day Initiative dari TippingPoint baru dimulai tahun 2005.

Baik iDefense maupun TippingPoint akan menyalurkan 0-day vulnerability yang dikumpulkan dari program kepada klien-klien mereka. Mereka yang membutuhkan informasi tersebut dapat dengan mudah ditebak. Mulai dari perusahaan pengembang produk **Intrusion Detection/Prevention System**, perusahaan pengembang produk **Security Assessment**, vendor sistem operasi dan aplikasi (demi mempercepat proses pencarian bugs), sampai pihak militer.

Selain dari para broker di atas, sudah mulai banyak **Security Researcher** yang membentuk perusahaan dan kemudian menjual sendiri hasil temuan mereka. Sebagai contoh adalah **ImmunitySec**, **CoreSecurity**, **Argeniss**, dan **Gleg**. Mereka mengemas 0-day vulnerability yang mereka temukan berikut metode eksploitasinya kedalam sebuah framework. Sebut saja Canvas dan Core Impact, yang ditawarkan ke publik sebagai produk yang dapat digunakan untuk security testing. Harga yang ditawarkan untuk framework yang berisi starter pack vulnerability mulai dari US\$ 1.000 sampai US\$ 15.000 dan untuk vulnerability pack ekstra yang berisi lebih banyak 0-day exploit mulai dari US\$ 2.000 sampai US\$ 10.000.

Walau pasar 0-day vulnerability sudah marak, forum-forum seperti Bugtraq, Full-Disclosure, Packetstorm,

Securiteam, dan Secunia tidak pernah sepi. Namun jika diperhatikan dengan baik, tidak banyak lagi hacker/cracker yang mau mempublikasikan informasi vulnerability yang sifatnya kritikal. Mereka lebih memilih untuk menyimpannya sendiri atau membagikannya ke rekan-rekan terdekat.

Sebut saja anggota-anggota dari geng ADM, TESO, THC, HERT, Gobbles, atau w00w00 yang sudah tidak lagi mempublikasikan hasil temuan mereka ke publik. Beberapa dari mereka malah sudah bergabung ke perusahaan sebagai Professional Security Researchers yang dibayar untuk mencari bugs dari sebuah sistem operasi atau aplikasi sebagai bagian dari Quality Assurance atau sebagai pendukung dari sebuah produk security.

## The Largest Information Security and Hacking Conference in Asia



# Bellua Cyber Security Asia 2006

## Second Annual Conference on Information Security & Hacking

**workshop : 28 - 29 August 2006**  
**Conference : 30 - 31 August 2006**

Jakarta Convention Center, Indonesia

**The main goal of the event is  
to increase security awareness  
& facilitate information sharing  
within the public, corporate  
and government sectors.**

# BELLUA ASIA PASIFIC Bellua Cyber Security Asia 2006

**Bellua Asia Pasific** meluncurkan event akbar yaitu **Bellua Cyber Security Asia 2006**, berlangsung mulai dari tanggal 28 sampai 31 Agustus. Sebagai pengenalan, NeoTek melakukan wawancara langsung saudara **Jim Geovedi** salah seorang dari tokoh penting di Bellua Asia Pasific.

**I**KUT..., TIDAK IKUT..., IKUT... RUGI BAGI YANG TIDAK ikutan acara Bellua Cyber Security Asia 2006 yang akan berlangsung pada bulan Agustus 2006 di Jakarta Convention Center.

Bellua Cyber Security Asia 2006 merupakan acara terbesar yang pernah diadakan di Indonesia, bahkan untuk Asia. Terbesar untuk acara yang memiliki informasi Security dan Hacking. Selain itu akan diadakan juga kompetisi CTF (Capture The Flag) yang dapat diikuti oleh siapa saja yang tertarik, tetapi tentu saja ada syarat yang harus dimiliki untuk mengikuti acaranya, yaitu terdaftar sebagai peserta di acara BCSA 2006.

Berikut merupakan wawancara kepada Jim Geovedi yang dilakukan NeoTek. Jim Geovedi dikenal sebagai pemerhati dan praktisi keamanan komputer dan internet, dan juga merupakan salah seorang dari tokoh penting di Bellua Asia Pasific.

Sebelum kita membahas lebih jauh mengenai seluk-beluk Bellua Cyber Security Asia 2006, pertama apa sih sebenarnya BCSA 2006?

Eit gw kasih flyernya dulu...

Yang jelas ini event tahunan kita yang kedua mengenai Information Security dan Hacking. Kita lebih mengarahkan kepada Knowledge Transfer melalui seminar dan conference tentang isu-isu keamanan yang sedang ngetrend.

Ok, pada event kali ini apa yang melatar belakangi diadakannya kembali Bellua Cyber Security Asia dan apakah kegiatan ini akan menjadi event rutin?

Kita mau jadi rutin! Di Indonesia belum ada yang spesifik bikin acara conference soal security yang tarafnya worldwide. Sementara ini masih banyak yang sifatnya lokal, seperti UIN, NEOTEK, atau anak-anak ECHO bikin acara itu kan masih sifatnya lokal. Sementara kita lebih worldwide dimana partisipan dari luar negeri juga banyak terus speakers-nya juga cukup banyak dari luar, jadi misalnya kamu punya hacker favorit bisa jadi nickname yang kamu maksud itu pernah ada atau akan ada.

Lalu apakah ada perbedaan dengan tahun yang lalu mas Jim?

Perbedaan yang signifikan, sekarang dunia security kebetulan dapat backup dari standar internasional, ada standar ISO 27001, dan itu baru dirilis beberapa bulan yang lalu, April.. eh sorry Maret. Kita akan angkat topik itu sebagai bagian dari compliance awarness, jadi compliance awarness itu lebih ke arah standar. Jadi bagaimana sebuah perusahaan me-manage Information Security di perusahaannya atau di instansinya, itu ada yang mengatur. Kita akan bahas banyak mengenai itu.

Kalau dari sisi technical, dimana-mana sama lah ya,

yang lagi ngetrend sekarang ini mobile application.

Dalam event Bellua Cyber Security Asia 2006, apa topik utama/tema yang akan diangkat dalam event tersebut?

Hm..., gak ada tema khusus, tapi issue yang diangkat adalah mengenai ISO standar, ISO 27001 itu, bahwa dengan adanya ISO tersebut setidaknya proses manajemen information security dalam suatu instansi bisa lebih baik.

Dengan melihat event BCS 2005 tahun lalu, kira-kira berapa peserta yang ditargetkan oleh panitia yang kemungkinan akan ikut berpartisipasi di acara Bellua Cyber Security tahun ini?

Kita sih ga muluk muluk yah, paling sekitar 400 sampai 600. Mungkin bisa lebih karena kita di JCC, kalau tahun lalu kan keterbatasan tempat.

Dari kalangan profesi apa saja yang menjadi target audience dalam event Bellua Cyber Security tahun ini?

Profesinya apa yah, orang-orang IT lah yang pasti, yang datang dikirim oleh perusahaannya. Bisa Admin-nya, IT Director-nya. Jadi apa yang membedakan BCS dengan conference yang lain adalah, disini kita membagi 2 (khusus untuk conference yah). Ada Business Track dan Technical Track. Jadi kalau ada orang teknis dia tidak akan harus merasa terpaksa di business track, dia cukup duduk aja di technical track. Sementara para manajer yang ikut mengerti teknis, bisa duduk di business track.

Apa yang ingin dicapai oleh Bellua sebagai salah satu perusahaan security di Indonesia dengan adanya acara BCS yang kedua kalinya ini?

Bellua tidak punya harapan apa-apa yang muluk, kita lebih ke awareness aja.

Melihat perkembangan teknologi yang semakin canggih sekarang ini, tingkat security threat pun semakin tinggi pula, nah bagaimana dengan tingkat security awareness di Indonesia?

Sudah mulai baik. Berkat media juga (majalah, radio, tv). Sudah banyak pengguna komputer yang sudah aware plus pengalaman pribadi dari orang tersebut yang mungkin pernah kena virus atau semacamnya, kemudian mereka mulai coba cari tahu gimana caranya supaya tidak kena virus dan akhirnya mereka mulai paham.

Awareness-nya sudah mulai bagus, hanya saja untuk beberapa level masih perlu ditingkatkan. Misalnya soal confidential data yang hanya untuk kalangan tertentu tapi ternyata masih disebarluaskan.

Ok, itu dari sisi enduser, lalu bagaimana di tingkat korporasi?

Malah mereka sudah lebih ketat, mereka sudah punya policy sendiri. Biasanya perusahaan-perusahaan tersebut sudah punya aturan/kebijaksanaan internal yang mana mereka mengatur organisasi security-nya sendiri di

dalam. Seperti bagaimana penggunaan email, internet, pembagian jaringan, bahkan untuk guide line penggunaan komputer mereka sudah punya.

Sekuriti dan kenyamanan adalah dua hal yang bertolak belakang, sebagai salah satu perusahaan sekuriti di Indonesia, apa pendapat Anda tentang kedua hal tersebut?

Oh..., bahkan di perusahaan perusahaan besar mereka juga mengalami masalah yang sama, salah satu rekomendasi yang kita berikan adalah memberikan training, bagaimana membuat password, dari hal-hal yang simple itu. Dan juga didukung dari setup system-nya. Jadi misalnya pada Windows Active Directory kita set supaya dalam periode tertentu harus ganti password, jadi ada password expired-nya.

Melihat perkembangan teknologi sekuriti komputer saat ini yang sudah semakin maju, boleh dong minta tipsnya mengenai apa aja yang seharusnya dilakukan oleh para pelaku IT khususnya para developer software untuk menghindari kesalahan pemrograman waktu mereka mendevlop software mereka?

Mau bicara scope Lokal apa Internasional nih?

Dari lokal dulu deh.

Satu deh tipsnya, jangan kebanyakan nyontek dari snippets orang. Karena apa? Kaya contohnya yang paling gampang, hmm apa yah..., mau bikin simple program dari PHP misalnya mau buat guestbook atau bikin blog software, trus function untuk connect ke MySQL-nya gak tau, trus liat-liat punya orang atau baca tutorial yang pernah ada di internet dan tanpa disadari kalo misalnya orang itu iseng bikin function dengan atau mungkin dia nulis function yang dimaksud tiga tahun yang lalu dan sekarang sudah harus dibenerin, berarti ada yang missing. Kita masih nyontek barang lama. Misalnya function eval() di PHP, kalo programmer PHP yang baru mulai, bisa jadi dia bawa bawa tuh function kemana-mana (ke program yang dia bikin). Padahal di PHP 5 mungkin sudah di hapuskan.

Terus untuk skala corporate, dalam mengembangkan aplikasi sebaiknya ada tim khusus yang ngurusin QC atau QA (Quality Control atau Quality Assurance) jadi tidak hanya fitur saja yang dipastikan harus ada tapi masalah security juga harus di-double check. Karena sering kali orang develop terus tidak ada QC, yang ada yang develop jadi QC sendiri hehe... Ketika ditanya bisa ini? Ada ini? Oh..., ada bisa... bisa..., ada!!! Tapi ketika ditanya security-nya gimana? Wah ntar dulu deh!

Menurut mas Jim, issue sekuriti apa yang sedang nge-trend di dunia industri?

Security issue? Hm..., kalo di media sih mulai dari urusan BotNet (red bukan BONET kan?) yee itu mah bogor net! Jadi BotNet itu kan robot network, jadi itu semacam program program yang ngendaliin/nguasain suatu komputer dan itu dihubungin jadi satu. Jadi bayangin ada remote admin, tau remote admin kan? (red: mudah-mudahan) dan remote admin itu dihubungkan jadi satu, jadi kamu cukup perintah satu command dan itu ada 1000, 2000, 3000, atau bahkan 1 juta komputer yang mengeksekusi perintah yang sama, dan jaringan pengontrol itu disebut botnet. Itu issue yang paling penting. Botnet itu kaya trojan, virus, agent yang nguasain komputer orang lain dan terkontrol pada suatu titik. Sampai botnet disebut sebagai sumber malapetaka, source of evil! Karena apa? Karena botnet bisa jadi spam relay, phishing scan, key logging, DOS itu udah jelas, porn

hosting. Mereka ter-distribute.

Dikalangan enduser khususnya di Indonesia, banyak dari mereka yang terjangkit virus lokal (contohnya brontok) dan itu jelas sangat mengganggu mereka, tapi apakah pada level korporasi hal ini juga terjadi?

Kalau dilokal itu masalah besar, banyak juga yang kena. Jelas mengganggu, karena nature-nya virus itu kalo nggak cuma numpang nama ya iseng gangguin orang! Cuma untungnya yang bikin brontok masih berbaik hati nggak bikin worm-nya, karena begitu dia bikin worm-nya, dia bisa nguasain hampir semua komputer di Indonesia, bukan tidak mungkin (yang basisnya Windows).

Kalau tidak salah nanti di acara BCS juga akan ada kompetisi hacking, bisa dijelaskan sedikit mengenai acara tersebut?

Hm..., prosedurnya adalah bikin tim terdiri dari beberapa orang dan bawa komputer sendiri. Kira kira 1 tim terdiri dari 3-5 orang.

Kita lagi menggodok aturannya, antara kita akan sediakan server untuk diserang rame-rame atau setiap tim diminta untuk setup sistemnya, bisa pake VMWare (atau sejenis) terus kita kasih iso dan mereka kemudian harus hardening itu (sistemnya) kemudian mereka akan saling menyerang satu sama lain.

Kalau soal level (tingkat kesulitan) apakah akan relatif sama atau diturunkan dari tahun 2005 kemarin?

Kemungkinan diturunkan, tapi tergantung, artinya begini, kalau kemarin targetnya centralized, dan aplikasinya yang digunakan tidak umum, jadi mereka (peserta) agak-agak repot. Tapi ternyata kalau sekarang misalnya kita temukan bahwa aplikasi yang akan kita pakai nanti umum disini kita akan pakai itu, jadi semacam web forum, mulai dari aplikasi yang simple seperti itu lah.

Apakah dibuka untuk umum juga?

Dibuka untuk umum, tapi tahun kemarin yang ikut kebanyakan yang udah pada kerja.

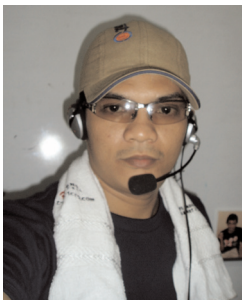
Biayanya berapa, apa akan sama seperti tahun lalu (gratis)?

Kemungkinan kita akan gratis...



Photo bersama Jim Geovedi (kiri) dan wartawan NeoTek, Rafeequl Rahman Awan (Kanan)





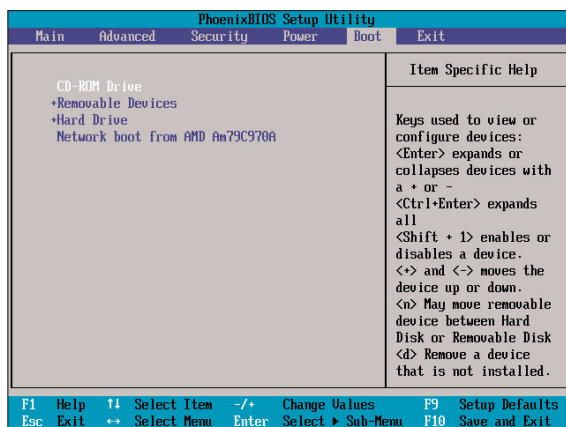
# PACERLINUX Menjalankan Live-CD

**Open Source Movement 2006** yang diusung oleh APKOMINDO dan didukung oleh PAZIA (distributor ACER di Indonesia untuk Aspire, Ferrari, dan LCD Monitor) meluncurkan distro baru PacerLinux. **MA Rody Candra** (support@pacerlinux.com) membahas seputar penggunaan PacerLinux.

**P**ACERLINUX LIVE-CD, MERASAKAN SEBUAH OPERATING System dengan hanya sebuah CD yang boot di komputer anda tanpa diperlukan sebuah instalasi. Walau hanya sebuah CD, PacerLinux hadir dengan kemampuan fitur-fitur yang baik, membuat anda seperti berada pada sebuah sistem operasi yang telah terinstalasi. Tidak membuktikannya mungkin belum membuat anda percaya, jadi buktikan saja.

Walaupun PacerLinux nantinya akan di-bundle pada produk Acer (Aspire maupun Ferrari), tetapi tidak menutup kemungkinan bagi anda yang tidak menggunakan produk komputer dari Acer tetap dapat mencoba PacerLinux.

**Setup Bios** pada opsi **Boot** adalah **CD ROM device**, tahap yang harus anda lakukan pertama kalinya. Tujuannya adalah ketika komputer pertama kali dinyalakan pada kondisi *warming up*, maka komputer akan membaca sistem yang berada pada CD untuk dijalankan.



Gambar 1. Setup bios pada opsi boot CD ROM device

Tekan F10 yang terdapat pada keyboard untuk menyimpan hasil setting dan keluar dari setup bios

Sebelum proses *warming up* berjalan, masukkan CD PacerLinux yang anda miliki ke CD ROM. Jika anda menemukan tampilan pada layar monitor komputer anda seperti yang ditunjukkan gambar 2, tekan saja **ENTER**.

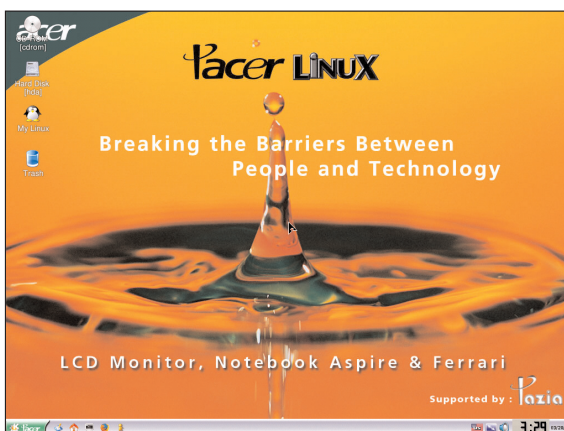
Tunggulah beberapa saat, proses-proses *loading* PacerLinux akan anda temui. Sampai seperti yang diperlihatkan pada gambar 4, anda sudah dapat menikmati PacerLinux sebagai Operating System yang Live-CD. Walaupun hanya Live-CD, anda sudah dapat menikmati berbagai aplikasi yang ada, termasuk aplikasi untuk surfing di internet dan chatting. Untuk dapat surfing dipastikan anda memiliki akses ke internet.



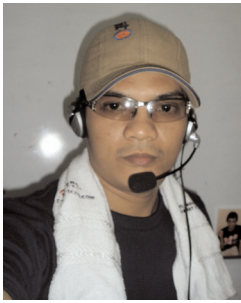
Gambar 2. Tekan Enter untuk memulai menjalankan PacerLinux



Gambar 4. Loading process



Gambar 5. PacerLinux Interface



# PACERLINUX Instalasi (Single Boot)

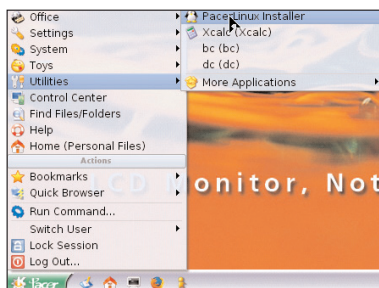
**Open Source Movement 2006** yang diusung oleh APKOMINDO dan didukung oleh PAZIA (distributor ACER di Indonesia untuk Aspire, Ferrari, dan LCD Monitor) meluncurkan distro baru PacerLinux. **MA Rody Candra** (support@pacerlinux.com) membahas seputar penggunaan PacerLinux.

**C** ACERLINUX LIVE-CD, MERASAKAN SEBUAH OPERATING System dengan hanya sebuah CD yang boot di komputer anda tanpa diperlukan sebuah instalasi. Walau hanya sebuah CD, PacerLinux hadir dengan kemampuan fitur-fitur yang baik, membuat anda seperti berada pada sebuah sistem operasi yang telah terinstalasi.

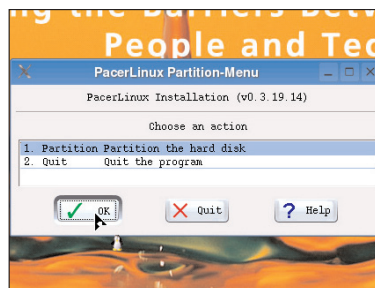
Tidak membuktikannya mungkin belum membuat anda percaya, jadi buktikan saja.

Walaupun PacerLinux nantinya akan di-bundle pada produk Acer (Aspire maupun Ferrari), tetapi tidak menutup kemungkinan bagi anda yang tidak menggunakan produk komputer dari Acer tetap dapat mencoba PacerLinux.

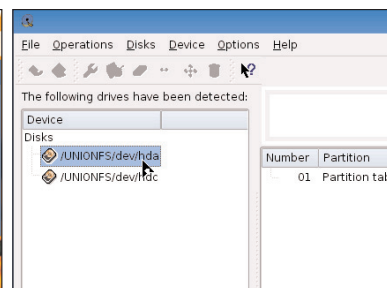
*Teknik instalasi PacerLinux ke dalam harddisk yang tidak terdapat Operating System lain*



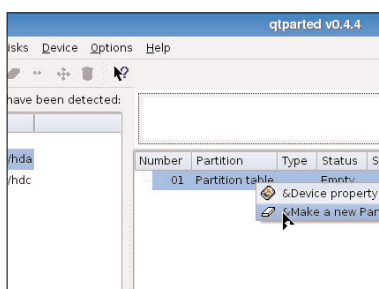
**1 PacerLinux installer**  
Aktifkan modul instalasi PacerLinux, mulai dari **Pacer>Utilities>PacerLinux Installer**. Selanjutnya anda akan menemui rangkaian window berisi informasi instalasi, klik OK untuk melanjutkan proses.



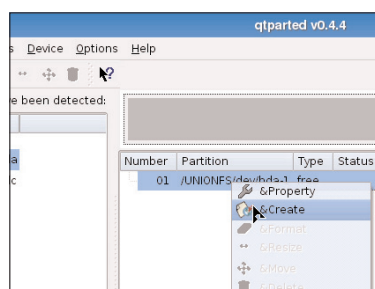
**2 Partition menu**  
Pada tahap ini anda diminta untuk memilih opsi yang pertama (1. Partition) yaitu **Partition the hard disk**. Selanjutnya klik OK, dan akan muncul **Window QTParted**.



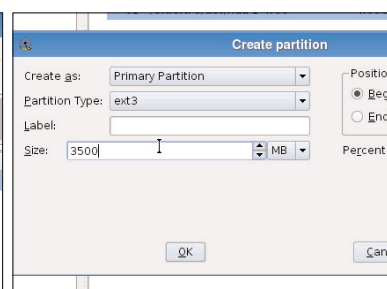
**3 Memilih harddisk device**  
Klik informasi harddisk yang terdeteksi pada frame kedua, pada frame kedua akan memperlihatkan informasi mengenai harddisk tersebut.



**4 New partition table**  
Dari informasi mengenai harddisk yang diperlihatkan pada frame kedua, anda perlu membuat table partisi. Lakukan klik kanan dan pilih opsi **&Make a new Partition Table**.

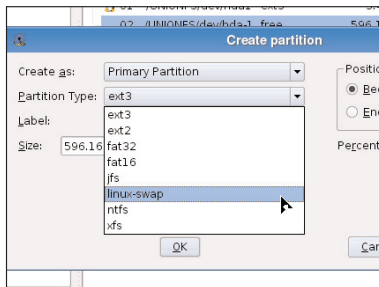


**5 Create partition**  
Untuk linux, diperlukan untuk membuat 2 partisi yaitu swap dan native. Untuk membuat partisi, klik kanan informasi harddisk yang ada pada frame 2 dan pilih opsi **&create**.



**6 Extended Partition**  
Buatlah terlebih dahulu partisi **extended** atau **native** (ext3). Kemudian tentukan ukuran partisi, sisakan space partisi minimal 500MB untuk partisi swap, kemudian klik OK.

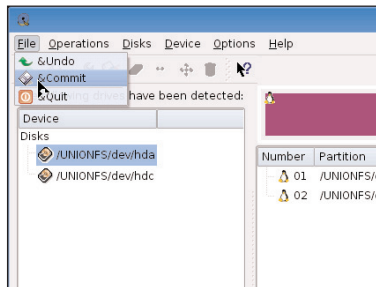
## NeoTutor



7

**Swap partition**

Sisa space partisi dibuat menjadi partisi swap, lakukan seperti langkah 5 untuk partisi free. Pada menu **Create Partition**, pilih opsi **Linux-swap** pada bagian **Partition Type**, kemudian klik **OK**.



8

**Commit**

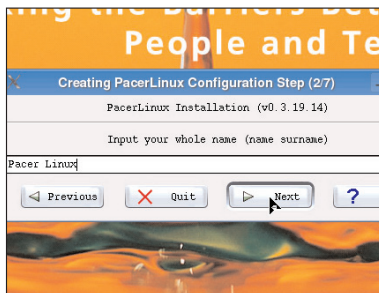
Setelah pembagian space partisi, satu langkah lagi untuk menyelesaikan bagian ini adalah melakukan commit. Dari menu **standard**, **File>Commit**



9

**QTParted warning!!!**

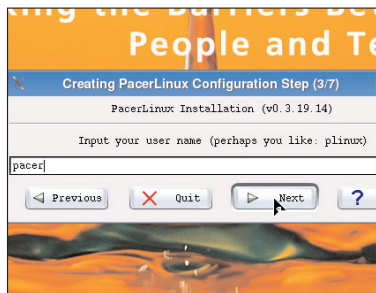
Ketika anda menjalankan perintah commit, akan muncul sebuah peringatan, lik tombol **YES** yang ada sebagai jawaban atas peringatan yang muncul tersebut.



13

**Input name**

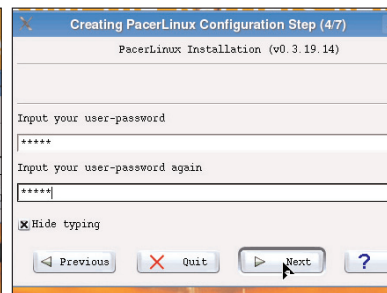
Konfigurasi kedua, memasukkan nama anda. Anda bisa memasukkan nama lengkap.



14

**Input username**

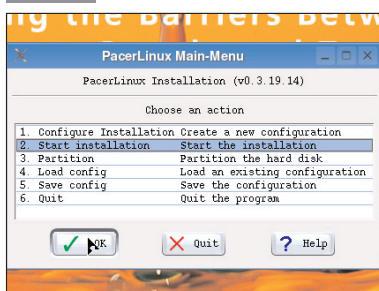
Konfigurasi ketiga, memasukkan nama pengguna PacerLinux nantinya (nama yang digunakan untuk mengakses PacerLinux), bisa menggunakan nama panggilan.



15

**Input user password**

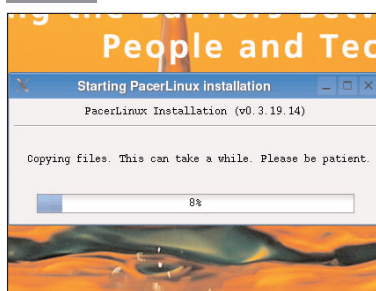
Konfigurasi keempat, memasukkan password yang akan digunakan oleh username yang telah anda tentukan untuk mengakses PacerLinux nantinya. *Jangan pernah melupakan password yang digunakan.*



19

**Start installation**

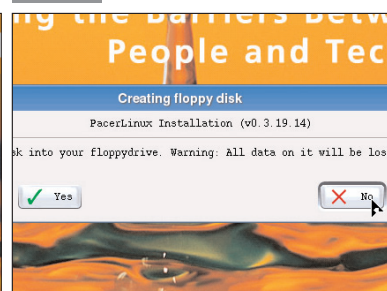
Kembali ke PacerLinux menu instalasi. Pilih opsi kedua yaitu **Start the installation**, maka instalasi PacerLinux akan dimulai.



20

**Proses instalasi**

Selama proses instalasi berlangsung, yang perlu anda lakukan adalah menunggu. Anda akan melihat seluruh proses yang terjadi seperti proses copying files.

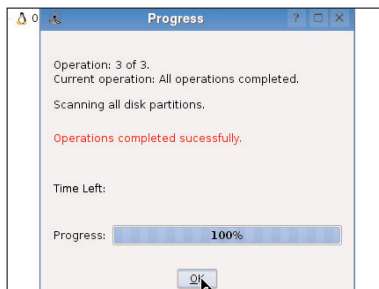


21

**Creating floppy disk**

Diakhir proses yaitu Creating floppy disk, disarankan anda menjawabnya dengan menekan tombol **No**. Instalasi selesai, restart komputer anda dan keluarkan CD PacerLinux.

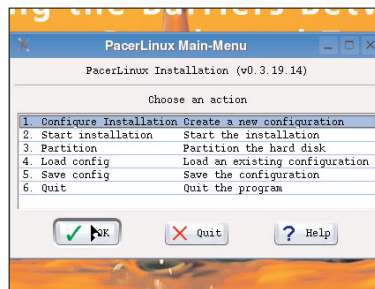




10

**Commit finish**

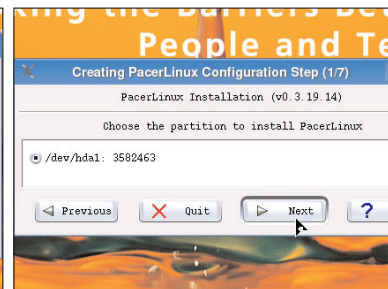
Ada beberapa proses yang berkaitan dengan commit, tungguhlah beberapa saat hingga proses selesai sepenuhnya. Ketika proses selesai klik tombol **OK**.



11

**New configuration**

Sesuai urusan pembagian partisi, tahapan selanjutnya adalah memilih **Configure Installation** yaitu **Create a new configuration** (opsi pertama).



12

**Memilih partisi**

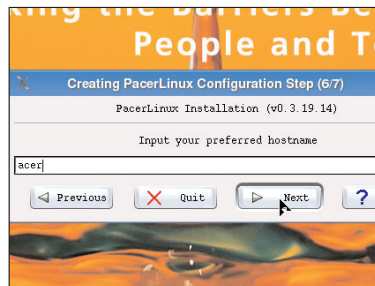
Konfigurasi pertama, pilih partisi yang akan digunakan untuk PacerLinux, tentu saja partisi extended yang anda pilih, klik **NEXT**. Masih di konfigurasi pertama, untuk pilihan filesystem, pilih opsi pertama yaitu **ext3**.



16

**Input admin password**

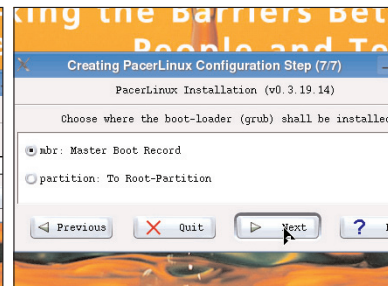
Konfigurasi kelima, memasukkan password administrator (root). Administrator adalah pengguna dengan level tertinggi yang dapat mengakses secara penuh PacerLinux nantinya.



17

**Input hostname**

Konfigurasi keenam, memasukkan hostname yang akan digunakan oleh PacerLinux anda. Anda bisa menentukannya sesuka hati atau sesuai dengan selera anda sendiri.



18

**Boot-loader**

Konfigurasi ketujuh, memilih boot-loader, dalam hal ini pilih opsi pertama yaitu **mbr: Master Boot Record**.

## Technical Support PacerLinux

B

AGI ANDA YANG MEMILIKI KESULITAN ATAU MASALAH ketika menggunakan PacerLinux, jangan ragu untuk menghubungi saudara **MA Rody Candra** (Redaktur Pelaksana NeoTek) yang telah ditunjuk sebagai Technical Support PacerLinux, kirim email berisikan masalah berkaitan dengan PacerLinux ke alamat email **support@pacerlinux.com**

Anda juga dapat bergabung di forum PacerLinux yang beralamat di **http://forum.pacerlinux.com**

Untuk nomor contact Technical Support PacerLinux belum ditentukan, masih dalam proses.

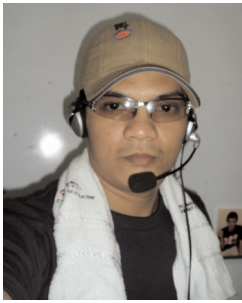
**Sekilas Mengenai PacerLinux**

PacerLinux merupakan singkatan dari **Pazia Acer Linux**, merupakan support nyata dari Pazia yang merupakan distributor produk ACER untuk Aspire, Ferrari, dan LCD Monitor, pada program **Open Source Movement 2006** yang diusung oleh **APKOMINDO**.

Untuk tahapan pertama, CD PacerLinux telah dicetak sebanyak 10.000 buah. Dan untuk membantu penggunaan PacerLinux, telah diterbitkan Buku Panduan PacerLinux (cetakan terbatas dan tidak diedarkan di toko-toko buku yang ada). Apa yang telah dibahas pada kesempatan edisi NeoTek kali ini, tidak selengkap seperti yang telah dibahas pada buku panduan PacerLinux. Untuk itu disarankan anda untuk memiliki buku tersebut.

Untuk pemesanan buku panduan PacerLinux, hubungi Ibu **Wulan** di alamat email **apkomindo@indo.net.id** dengan subject email **Buku Panduan PacerLinux**.

Mulai awal Juni 2006, akan diadakan pelatihan pengoperasian PacerLinux, yang dilaksanakan Mall to Mall dan di 6 DPD Apkomindo. Informasi lebih jelas akan diberitakan di forum PacerLinux.



# PACERLINUX Instalasi (Dual Boot)

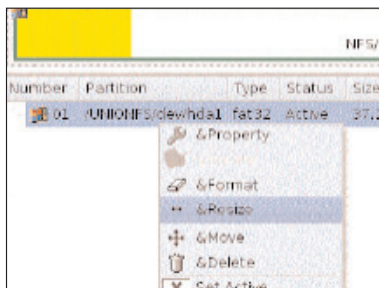
**Open Source Movement 2006** yang diusung oleh APKOMINDO dan didukung oleh PAZIA (distributor ACER di Indonesia untuk Aspire, Ferrari, dan LCD Monitor) meluncurkan distro baru PacerLinux. **MA Rody Candra** (support@pacerlinux.com) membahas seputar penggunaan PacerLinux.

**C** ACERLINUX LIVE-CD, MERASAKAN SEBUAH OPERATING System dengan hanya sebuah CD yang boot di komputer anda tanpa diperlukan sebuah instalasi. Walau hanya sebuah CD, PacerLinux hadir dengan kemampuan fitur-fitur yang baik, membuat anda seperti berada pada sebuah sistem operasi yang telah terinstalasi.

Tidak membuktikannya mungkin belum membuat anda percaya, jadi buktikan saja.

Walaupun PacerLinux nantinya akan di-bundle pada produk Acer (Aspire maupun Ferrari), tetapi tidak menutup kemungkinan bagi anda yang tidak menggunakan produk komputer dari Acer tetap dapat mencoba PacerLinux.

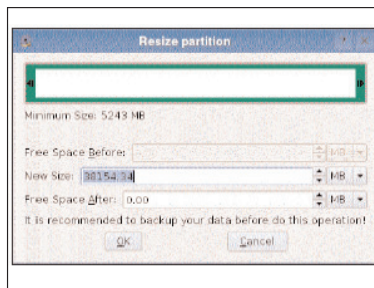
*Teknik instalasi PacerLinux ke dalam harddisk yang telah terdapat Microsoft Windows*



## 4

### Resize (1)

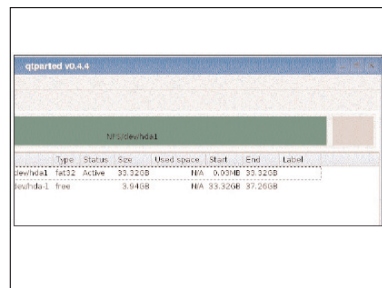
Pada informasi harddisk device di frame kedua, lakukan klik kanan untuk memunculkan menu dan pilih opsi **&Resize**.



## 5

### Resize (2)

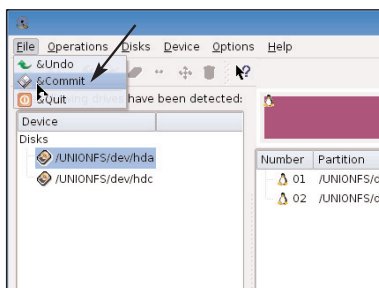
Anda dapat menentukan nilai space harddisk dengan mengetikkan langsung di box isian **New Size**, atau dengan cara lain yaitu menarik kotak hijau dari sebelah kanan ke kiri. Jika sudah selesai, klik **OK**.



## 6

### Contoh hasil resize

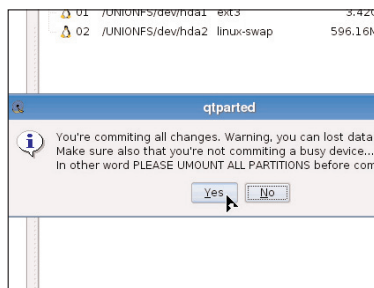
Klik informasi harddisk yang terdeteksi pada frame kedua akan memperlihatkan informasi mengenai harddisk tersebut.



## 10

### Commit

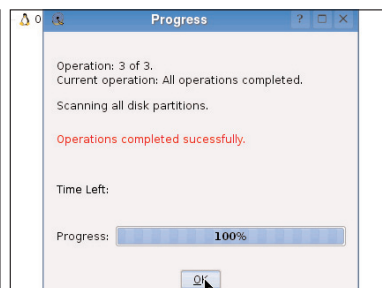
Setelah pembagian space parti, satu langkah lagi untuk menyelesaikan bagian ini adalah melakukan commit. Dari menu standard, **File>Commit**



## 11

### QTParted warning!!!

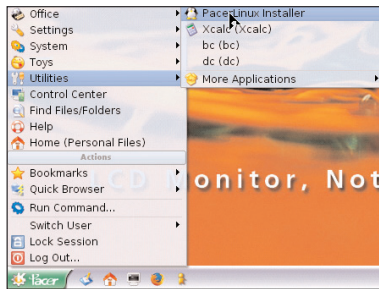
Ketika anda menjalankan perintah commit, akan muncul sebuah peringatan, lik tombol **YES** yang ada sebagai jawaban atas peringatan yang muncul tersebut.



## 12

### Commit finish

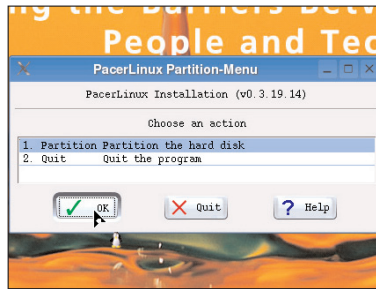
Ada beberapa proses yang berkaitan dengan commit, tungguilah beberapa saat hingga proses selesai sepenuhnya. Ketika proses selesai klik tombol **OK**.



1

**PacerLinux installer**

Aktifkan modul instalasi PacerLinux, mulai dari **Pacer>Utilities>PacerLinux Installer**. Selanjutnya anda akan menemui rangkaian window berisi informasi instalasi, klik OK untuk melanjutkan proses.



2

**Partition menu**

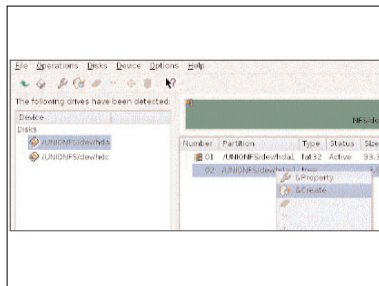
Pada tahap ini anda diminta untuk memilih opsi yang pertama (1. Partition) yaitu **Partition the hard disk**. Selanjutnya klik OK, dan akan muncul **Window QTParted**.



3

**Memilih harddisk device**

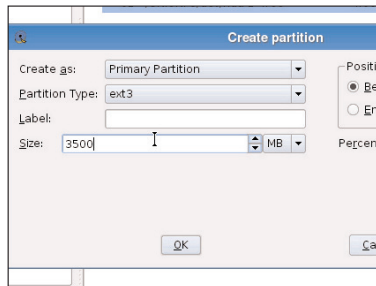
Klik informasi harddisk yang terdeteksi pada frame pertama, pada frame kedua akan memperlihatkan informasi mengenai harddisk tersebut.



7

**Create partition**

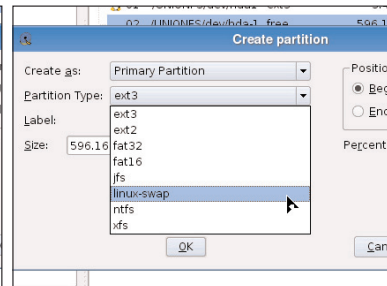
Untuk linux, diperlukan untuk membuat 2 partisi yaitu swap dan native. Untuk membuat partisi, klik kanan informasi harddisk yang ada pada frame 2 dan pilih opsi **&create**.



8

**Extended Partition**

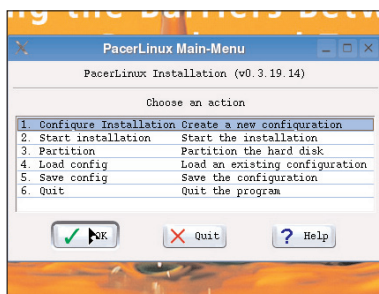
Buatlah terlebih dahulu partisi **extended** atau **native** (ext3). Kemudian tentukan ukuran partisi, sisakan space partisi minimal 500MB untuk partisi swap, kemudian klik OK.



9

**Swap partition**

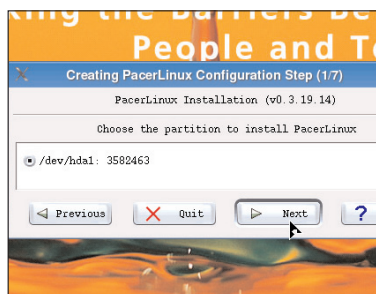
Sisa space partisi dibuat menjadi partisi swap, lakukan seperti langkah 7 untuk partisi free. Pada menu **Create Partition**, pilih opsi **Linux-swaps** pada bagian **Partition Type**, kemudian klik OK.



13

**New configuration**

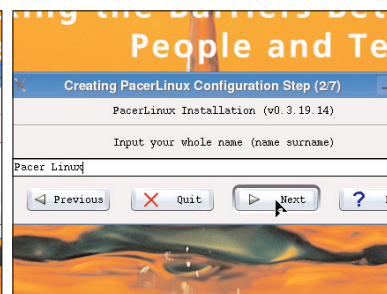
Selesai urusan pembagian partisi, tahapan selanjutnya adalah memilih **Configure Installation** yaitu **Create a new configuration** (opsi pertama).



14

**Memilih partisi**

Konfigurasi pertama, pilih partisi yang akan digunakan untuk PacerLinux, tentu saja partisi extended yang anda pilih, klik **NEXT**. Masih di konfigurasi pertama, untuk pilihan filesystem, pilih opsi pertama yaitu **ext3**.



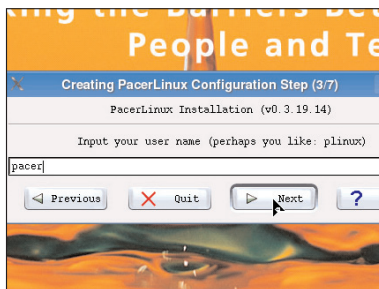
15

**Input name**

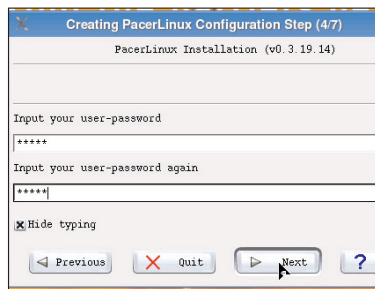
Konfigurasi kedua, memasukkan nama anda. Anda bisa memasukkan nama lengkap.



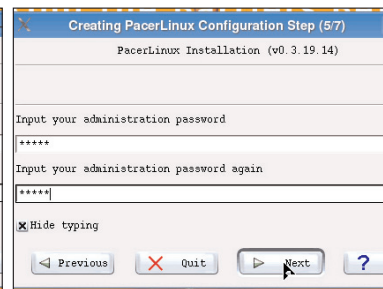
## NeoTutor



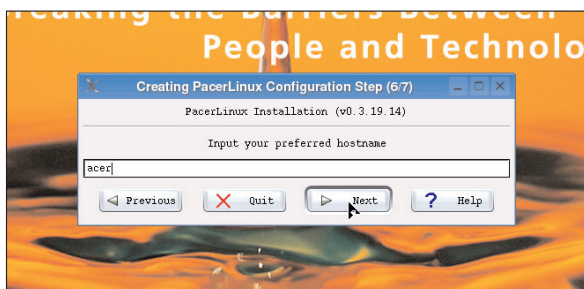
**16 Input username**  
Konfigurasi ketiga, memasukkan nama pengguna PacerLinux nantinya (nama yang digunakan untuk mengakses PacerLinux), bisa menggunakan nama panggilan.



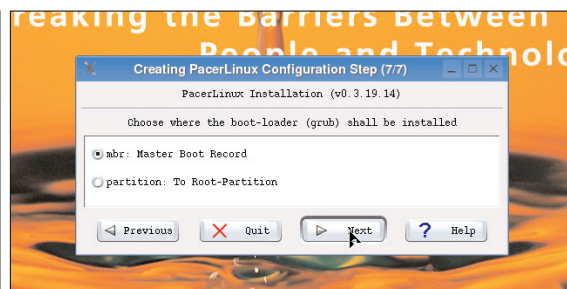
**17 Input user password**  
Konfigurasi keempat, memasukkan password yang akan digunakan oleh username yang telah anda tentukan untuk mengakses PacerLinux nantinya. *Jangan pernah melupakan password yang digunakan.*



**18 Input admin password**  
Konfigurasi kelima, memasukkan password administrator (root). Administrator adalah pengguna dengan level tertinggi yang dapat mengakses secara penuh PacerLinux nantinya.



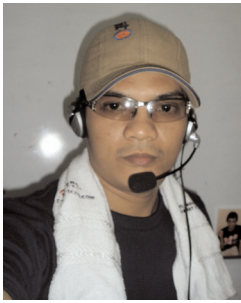
**19 Input hostname**  
Konfigurasi keenam, memasukkan hostname yang akan digunakan oleh PacerLinux anda. Anda bisa menentukannya sesuka hati atau sesuai dengan selera anda sendiri.



**20 Boot-loader**  
Konfigurasi ketujuh, memilih boot-loader, dalam hal ini pilih opsi pertama yaitu **mbr: Master Boot Record**.



Forum yang khusus membahas mengenai PacerLinux



# PACERLINUX Aplikasi Pendukung

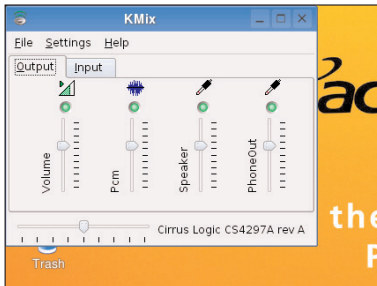
**Open Source Movement 2006** yang diusung oleh APKOMINDO dan didukung oleh PAZIA (distributor ACER di Indonesia untuk Aspire, Ferrari, dan LCD Monitor) meluncurkan distro baru PacerLinux. **MA Rody Candra** (support@pacerlinux.com) membahas seputar penggunaan PacerLinux.

**A**PLIKASI-APLIKASI (SOFTWARE) PENDUKUNG YANG ADA di pacerLinux dapat dijalankan, baik dalam kondisi sebagai Live-CD maupun telah terinstallasi ke dalam harddisk.

Aplikasi apa saja yang terdapat di PacerLinux? Berikut ini

beberapa aplikasi yang dapat anda temukan nantinya yang kegunaan mungkin biasa anda gunakan dalam kehidupan sehari-hari ketika berhadapan dengan komputer. Untuk aplikasi lain-lainnya, sebaiknya anda mencari tahu sendiri, untuk itu jangan menunggu lagi untuk menggunakan PacerLinux.

*Beberapa aplikasi yang didukung oleh PacerLinux*



**1**

## KMix

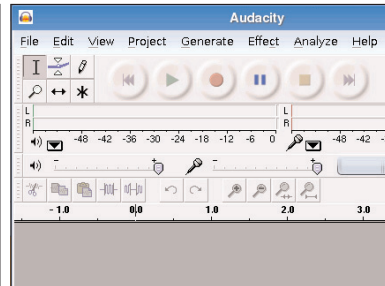
Jika di Microsoft Windows ada Volume Control, maka di PacerLinux ada KMix. Fungsinya sama yaitu sebagai pengaturan/kontrol terhadap sound.



**2**

## XMMS

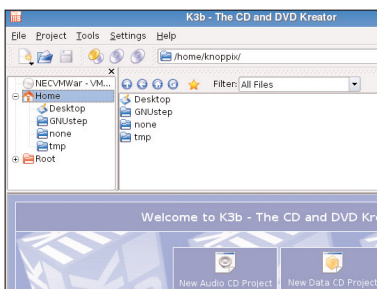
Untuk memutar MP3 biasa menggunakan program WinAmp, maka ketika bertemu XMMS tidak akan membuat anda menjadi asing karena XMMS hampir mirip dengan WinAmp.



**3**

## Audacity

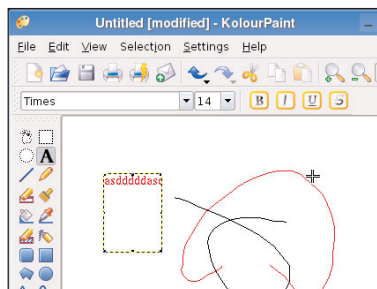
Punya hobby mengedit musik atau menggabungkan beberapa musik atau membuat efek sound? Program ini yang akan memuaskan hobby anda tersebut.



**4**

## K3b

Biasa menggunakan program Nero untuk membakar CD ataupun DVD, di PacerLinux anda akan bertemu dengan K3b untuk melakukan tugas bakar membakar CD atau DVD.



**5**

## KolourPaint

Nyaris mirip dengan program Paint yang terdapat di Microsoft Windows, kelebihanannya adalah interface yang lebih menarik dipandang mata.

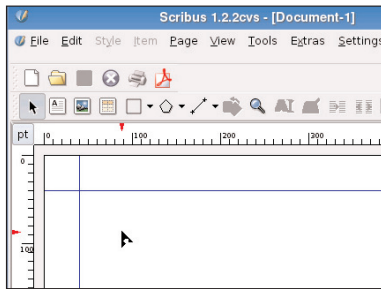


**6**

## KSnapshot

Untuk urusan tangkap-menangkap screen atau bagian tertentu dari screen, maka KSnapshot hadir sebagai solusinya.

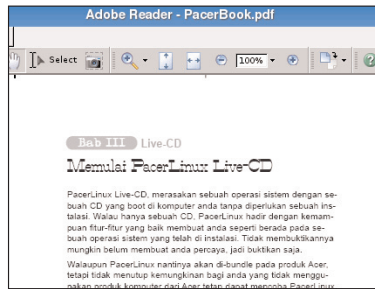
## NeoTutor



# 7

### Scribus

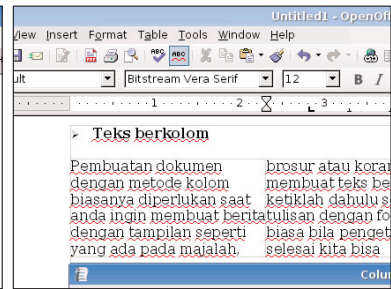
Bekerja sebagai editor di surat kabar atau majalah, dibutuhkan program editor yang dapat membantu pekerjaan editing, scribus hadir sebagai jawabannya.



# 8

### Adobe Reader

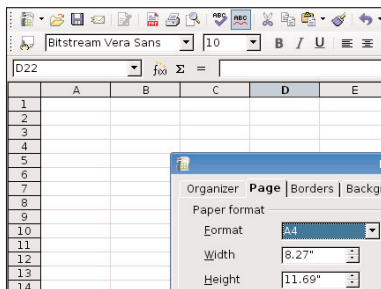
Membaca file PDF di PacerLinux menjadi semakin mudah karena telah tersedia Adobe Reader. Tidak perlu bersusah melakukan instalasi karena memang telah tersedia.



# 9

### OpenOffice.org Writer

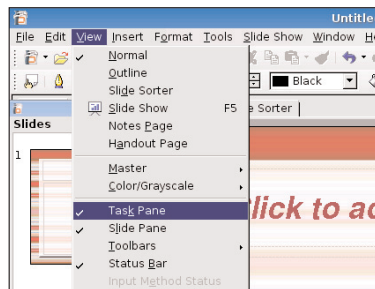
Program pengolahan kata ini fungsinya sama seperti Microsoft Word. Bagi yang terbiasa menggunakan Microsoft Word, maka tidak akan asing ketika menggunakan OpenOffice.org Writer.



# 10

### OpenOffice.org Calc

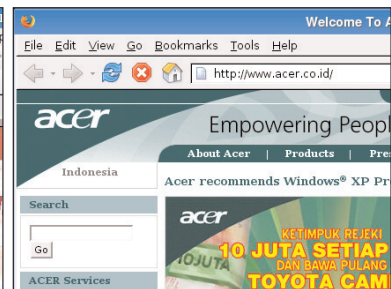
Selain OpenOffice.org Witer, ada lagi program yang memiliki fungsi sama seperti halnya Microsoft Excel yaitu OpenOffice.org Calc.



# 11

### OpenOffice.org Impress

Untuk urusan presentasi yang biasa dibuat di Microsoft Powerpoint, di PacerLinux tersedia OpenOffice.org Impress.



# 12

### Firefox Browser

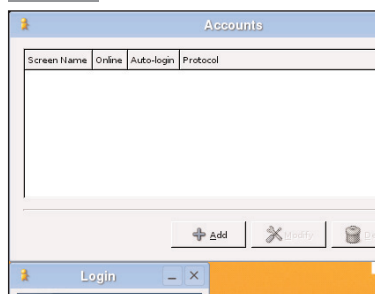
Berkelana di dunia maya menggunakan Mozilla Firefox, kemampuannya tidak kalah dengan Internet Explorer Browser, bahkan Mozilla Firefox memiliki plugin-plugin yang banyak tersedia di Internet.



# 13

### Konqueror Browser

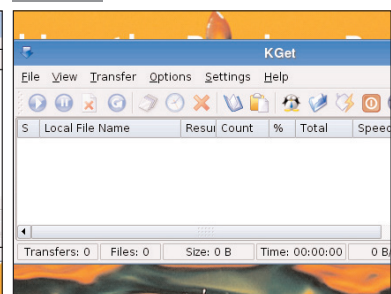
Selain Mozilla Firefox, juga tersedia Konqueror Browser untuk urusan berkelana di dunia maya, kemampuannya juga tidak kalah saing dengan Mozilla Firefox.



# 14

### Gaim Messenger

Chatting jadi semakin asyik menggunakan Gaim Messenger, mulai dari chat Yahoo! Messenger, mIRC, dan lain-lain dilakukan dalam satu window.

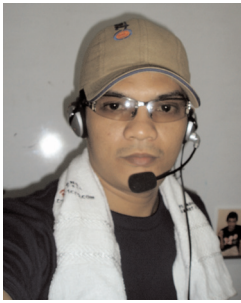


# 15

### Download Manager

Senang men-download file-file baik berupa MP3, film, gambar, dan lain-lain, manfaatkan program ini. Urusan download menjadi lebih asyik.





# PACERLINUX Network dan Printer

**Open Source Movement 2006** yang diusung oleh APKOMINDO dan didukung oleh PAZIA (distributor ACER di Indonesia untuk Aspire, Ferrari, dan LCD Monitor) meluncurkan distro baru PacerLinux. **MA Rody Candra** (support@pacerlinux.com) membahas seputar penggunaan PacerLinux.

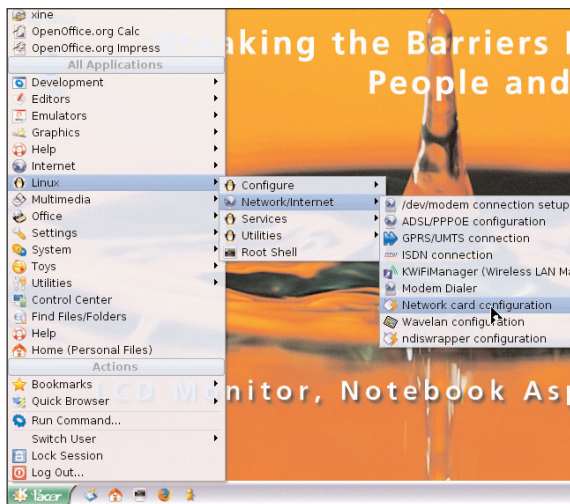
**J**IKA ANDA BERKUTAT DENGAN JARINGAN BAIK DI kantor maupun di rumah, dalam uji coba yang dilakukan PacerLinux memberikan kemudahan untuk urusan yang berkaitan dengan jaringan sehingga hanya dalam beberapa menit komputer anda yang menggunakan PacerLinux dapat tergabung dalam jaringan.

Device-device jaringan keluaran terbaru saat ini, mendapatkan perhatian yang serius oleh PacerLinux sehingga terkadang tanpa perlu konfigurasi PacerLinux anda sudah dapat bergabung dalam jaringan. Untuk itu bahasan mengenai jaringan hadir pada bab ini untuk mengatasi kendala yang mungkin saja anda temukan ketika berhadapan dengan urusan jaringan.

Selain itu, pada bab ini juga akan membahas mengenai printer. Penggunaan printer yang cukup luas di masyarakat membuat PacerLinux mencoba menyuguhkan berbagai driver dari berbagai merek dan tipe mesin printer, tidak lengkap tapi cukup begitu lengkap.

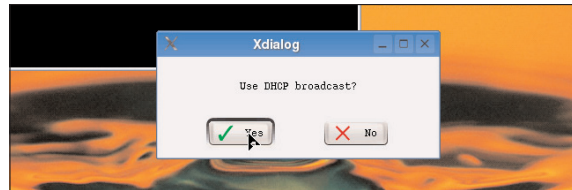
## Jaringan Kabel

Agar komputer anda yang menggunakan PacerLinux terkoneksi dengan jaringannya, cara sangat mudah. Aktifkan modul **Network Card** yang dapat anda tekan di **Pacer>Linux>Network/Internet>Network card configuration**.



Gambar 1. Network card configuration

Modul network card akan muncul dan sebuah **Xdialog** yang menanyakan apakah jaringan anda menggunakan DHCP (Dynamic Host Configuration Protocol), pilih **YES** jika jaringan anda menggunakan DHCP dan pilih **NO** jika tidak menggunakannya.

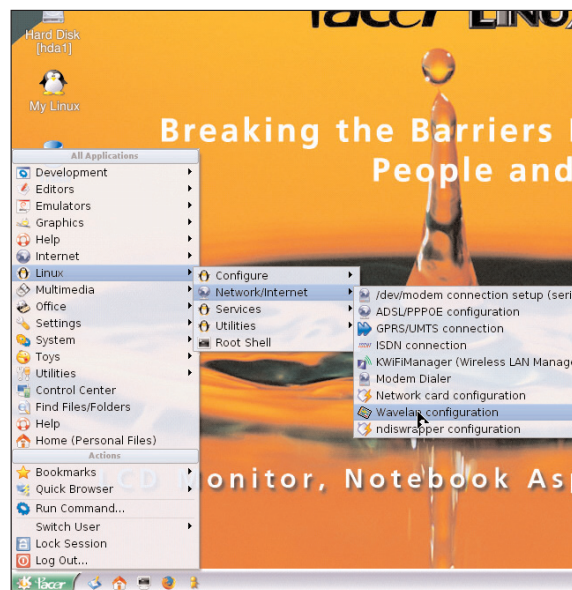


Gambar 2. Xdialog; DHCP

Ketika proses konfigurasi dimulai karena pertanyaan awal Xdialog, jika jaringan anda menggunakan DHCP maka konfigurasi akan segera ditangani oleh modul network card secara otomatis, tetapi jika tidak maka anda akan menemui beberapa pertanyaan dari Xdialog, ikuti dan isi sesuai dengan konfigurasi jaringan yang anda miliki.

## Jaringan WiFi

Jika komputer anda memiliki **WiFi**, aktifkan modul **Wavelan** yang dapat anda temukan di **Pacer>Linux>Network/Internet>Wavelan**.



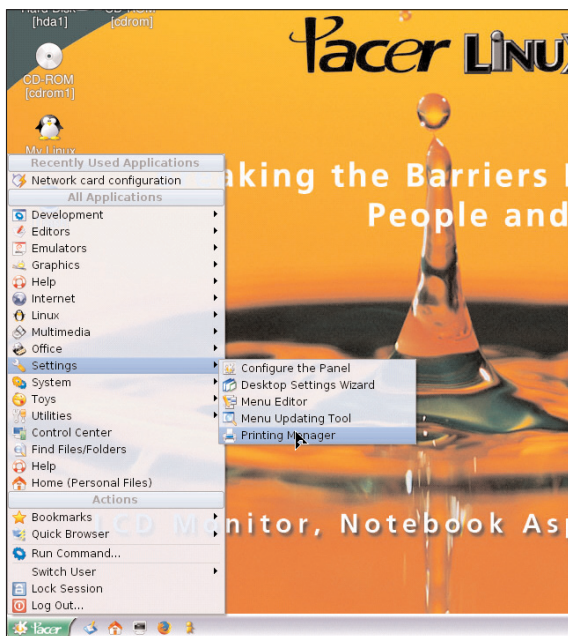
Gambar 3. Wavelan configuration

Seperti halnya dengan konfigurasi network card, hal pertama yang akan ditemukan yaitu pertanyaan **YES or NO** dari Xdialog akan penggunaan DHCP. Baik menjawab **YES** atau **NO**, anda akan menemui beberapa pertanyaan lainnya yang memerlukan jawaban, isilah sesuai keadaan konfigurasi jaringan anda (IP, ESSID, CHANNEL, dan lain-lain).

## Printer

Banyak orang yang mengalami kesulitan ketika berhadapan dengan urusan driver atas mesin printer yang dimilikinya, hal itu membuat orang menjadi enggan berurusan dengan Linux. Ada lagi orang yang masih ingin mencoba bersentuhan akan hal tersebut yang mencoba mencari solusi di internet, ketika driver didapat kembali menemukan permasalahan karena kesulitan ketika melakukan instalasi dan konfigurasinya.

PacerLinux menyadari akan hal yang disebutkan di atas, oleh sebab itu PacerLinux menawarkan kemudahan. Cukup melakukan klik dan klik permasalahan selesai. Kelebihan lainnya yang ditawarkan oleh PacerLinux tidak hanya untuk mesin printer yang berada dalam port lokal (local port), untuk mesin printer yang berada dalam sebuah jaringan dan telah di-share penggunaannya dapat digunakan tanpa harus menyambungkan mesin printer langsung ke komputer anda yang menggunakan PacerLinux. Aktifkan modul **Printer Manager** yang dapat anda temukan di **Pacer Start>Settings> Printing Manager**.



Gambar 4. Printing manager module

### Local Printer

Sebelum memulai konfigurasi, pastikan kabel printer telah terhubung dengan komputer anda dan power printer telah menyala. Ikuti langkah-langkah berikut ini.

#### Aktifkan modul Printing Manager.

Untuk langkah ini perhatikan gambar 4 di atas.

#### Add Printer.

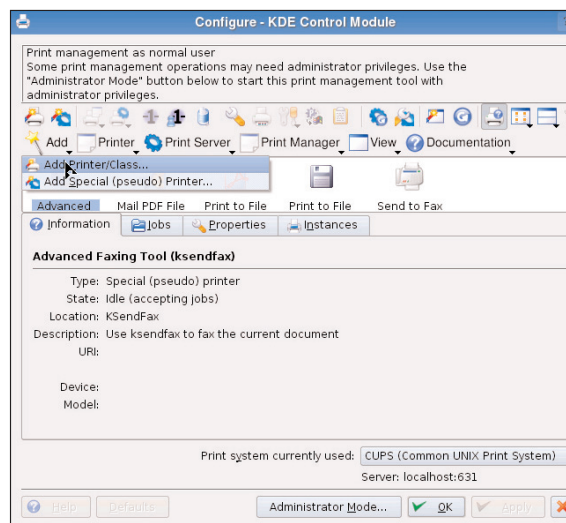
Klik tombol **Add** dan pilih opsi pertama **Add Printer/Class**, gambar 5.

#### Introduction.

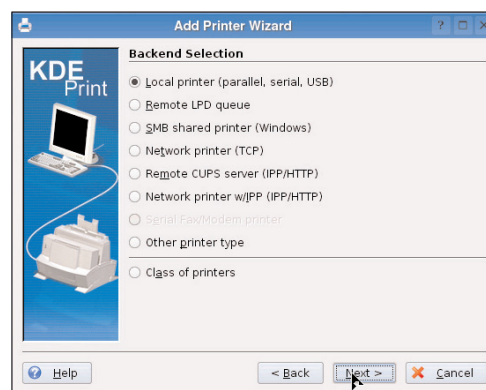
Ketika menu Introduction muncul, yang perlu anda lakukan hanya klik tombol **NEXT**.

#### Backend Selection.

Pilih opsi pertama yaitu **Local Printer (parallel, serial, USB)**, kemudian klik **NEXT**, gambar 6.



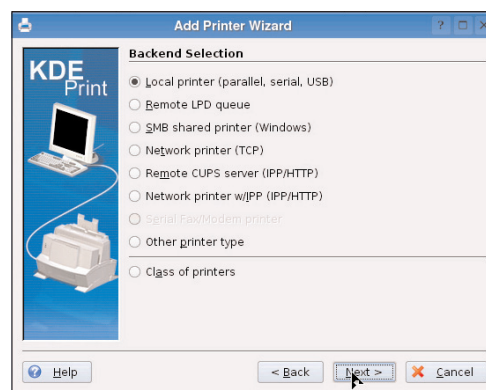
Gambar 5. Add printer



Gambar 6. Backend Selection

### Local Port Selection.

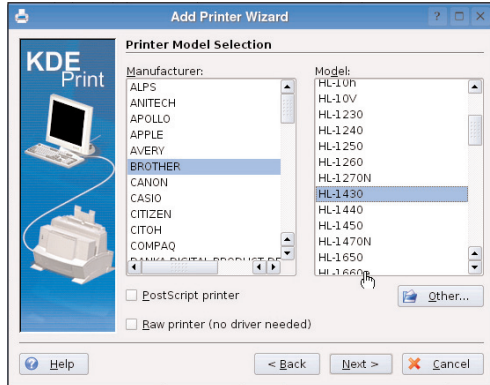
Pada local port selection, pilihlah jenis sambungan yang digunakan printer ke komputer anda, pada contoh printer yang digunakan tersambung ke komputer melalui USB. Klik **NEXT** untuk melanjutkan konfigurasi.



Gambar 7. Local port selection

**Printer Model Selection.**

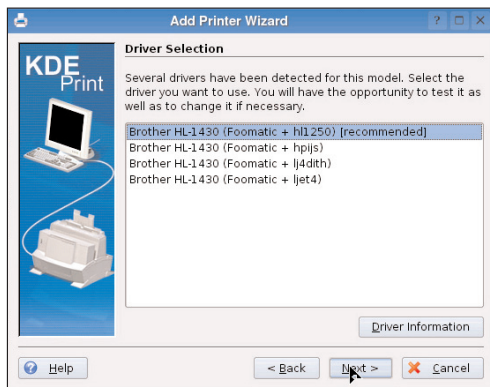
Pada tahap ini, pilih manufacture dan model dari mesin printer yang sesuai milik anda. Kembali klik NEXT untuk melanjutkan konfigurasi.



Gambar 8. Printer model selection

**Driver Selection.**

Setelah mendapatkan **manufacture** dan **model** yang sesuai dengan printer yang anda miliki, selanjutnya adalah pemilihan **driver**-nya, pilih opsi yang di rekomendasikan (recommended).



Gambar 9. Driver selection

**Banner Selection.**

Pada tahap ini anda cukup klik NEXT untuk melanjutkan konfigurasi.

**Printer Quota Settings.**

Kembali melakukan hal sama yaitu klik NEXT, anda tidak perlu melakukan settingan tertentu.

**Users Access Settings.**

Pada tahap ini, anda dapat menambahkan hak akses terhadap user yang boleh dan tidak boleh menggunakan printer. Tetapi lebih disarankan anda tidak perlu menambahkan sesuatu apapun, cukup klik NEXT.

**General Information.**

Anda dapat memberikan nama mesin printer yang anda gunakan dengan nama sesuai selera, setelah itu klik NEXT.

**Confirmation.**

Konfigurasi selesai, klik FINISH.

**Quit.**

Akhiri konfigurasi anda sepenuhnya dengan keluar dari modul **Printer Manager**.

**Windows Network Printer**

Bagaimana dengan mesin printer yang berada dalam jaringan? Tidak ada yang perlu dirisaukan, yang terpenting komputer anda telah terkoneksi dalam jaringan. Cara konfigurasi hanya berbeda pada beberapa langkah yang berada diawal, selanjutnya nanti sama. Tetapi agar tidak membingungkan anda, semua langkah akan tetap tersaji di bawah ini.

**Aktifkan modul Printing Manager.****Add Printer.**

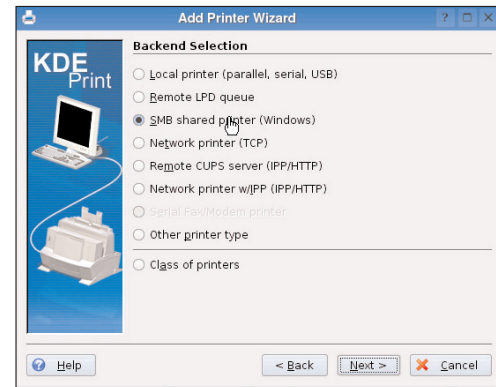
Klik tombol **Add** dan pilih opsi pertama **Add Printer/Class**.

**Introduction.**

Ketika menu Introduction muncul, yang perlu anda lakukan hanya klik tombol NEXT.

**Backend Selection.**

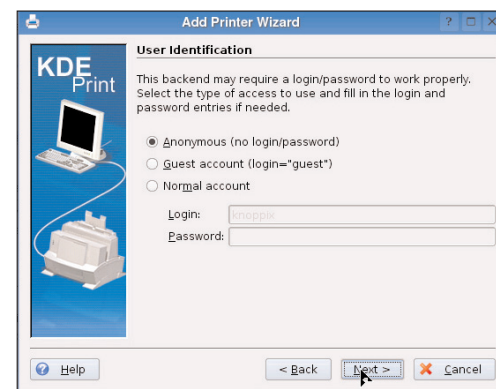
Pilih opsi pertama **SMB shared printer (Windows)**, kemudian klik NEXT.



Gambar 10. Backend Selection

**User Identification.**

Pilih opsi pertama yaitu **Anonymous (no login/password)**, kemudian klik NEXT.

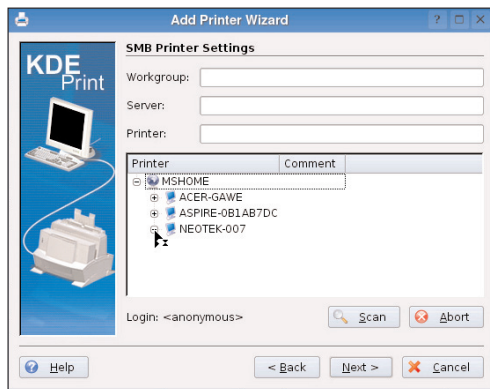


Gambar 11. User Identification

**SMB Printer Settings.**

Pada tahapan ini, lakukan scan terhadap mesin printer yang telah di-share pada jaringan. Hasil scan dapat terlihat pada frame printer, pilihlah komputer dimana mesin printer yang di-share berada.





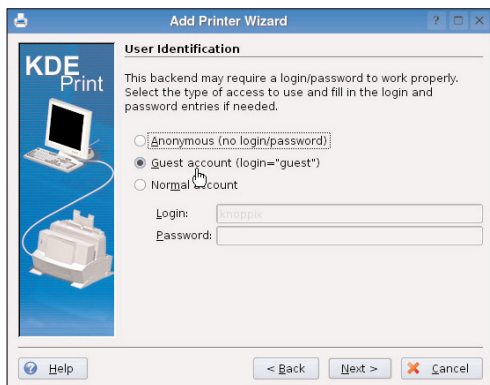
Gambar 12. SMB printer settings

Jika anda menemui peringatan seperti yang diperlihatkan pada gambar di bawah, klik saja OK.



Gambar 13. Access denied

Karena di Windows mengenal akses **Guest** dan tidak mengenal akses **Anonymous**, maka peringatan seperti yang ditunjukkan gambar 13 muncul. Jadi akses anonymous hanya digunakan untuk scan printer di jaringan, karena di Linux lebih mengenal akses Anonymous dibanding Guest. Oleh sebab itu klik BACK sehingga anda akan dibawa ke **User Identification**, pilih opsi kedua **Guest account** (login="guest"), kemudian klik NEXT.

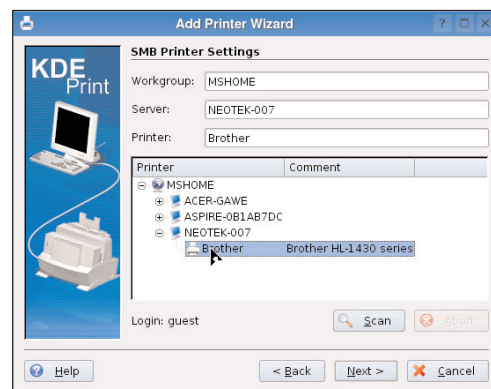


Gambar 14. Mengganti User identification ke guest

Kembali anda akan berada di tahapan **SMB Printer Settings**. Klik komputer dimana mesin printer yang telah di-share berada, maka anda akan melihat muncul *icon* yang menandakan mesin printer yang ada pada komputer tersebut siap tersambung dengan komputer anda. Klik NEXT untuk melanjutkan konfigurasi, perhatikan gambar 15.

#### Printer Model Selection.

Pada tahap ini, pilih **manufacture** dan **model** dari mesin printer yang sesuai milik anda. Kembali klik NEXT untuk melanjutkan konfigurasi.



Gambar 15. Kembali ke SMB printer settings

#### Driver Selection.

Setelah mendapatkan manufacture dan model yang sesuai dengan printer yang anda miliki, selanjutnya adalah pemilihan *driver*-nya, pilih opsi yang di rekomendasikan (recommended).

#### Banner Selection.

Pada tahap ini anda cukup klik NEXT untuk melanjutkan konfigurasi.

#### Printer Quota Settings.

Kembali melakukan hal sama yaitu klik NEXT, anda tidak perlu melakukan settingan tertentu.

#### Users Access Settings.

Pada tahap ini, anda dapat menambahkan hak akses terhadap user yang boleh dan tidak boleh menggunakan printer. Tetapi lebih disarankan anda tidak perlu menambahkan sesuatu apapun, cukup klik NEXT.

#### General Information.

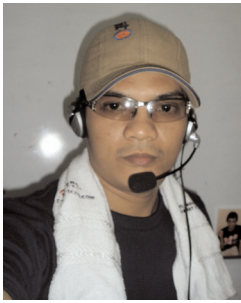
Anda dapat memberikan nama mesin printer yang anda gunakan dengan nama sesuai selera, setelah itu klik NEXT.

#### Confirmation.

Konfigurasi selesai, klik FINISH.

#### Quit.

Akhiri konfigurasi anda sepenuhnya dengan keluar dari modul **Printer Manager** dengan klik OK.



# PACERLINUX Samba Network

**Open Source Movement 2006** yang diusung oleh APKOMINDO dan didukung oleh PAZIA (distributor ACER di Indonesia untuk Aspire, Ferrari, dan LCD Monitor) meluncurkan distro baru PacerLinux. **MA Rody Candra** (support@pacerlinux.com) membahas seputar penggunaan PacerLinux.

**P**ACERLINUX JUGA DAPAT MELAKUKAN FILE SHARING dengan komputer lain yang menggunakan Operating System Microsoft Windows. Untuk itu diperlukan paket Sambar Network Neighbourhood yang telah dipaketkan dalam PacerLinux.

## Persiapan

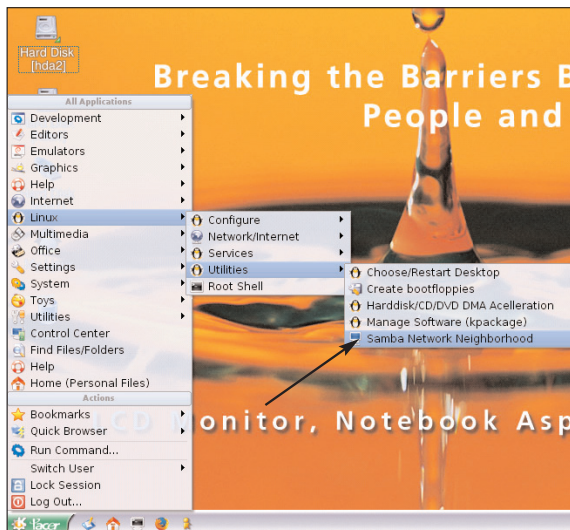
Syarat-syarat yang harus dipenuhi sebelum mencoba fasilitas Samba Network Neighbourhood, adalah:

- Pastikan berada dalam sebuah jaringan.
- PacerLinux anda telah dikonfigurasi atau tersambung dalam jaringan.
- Salah satu atau lebih, komputer yang memiliki Operating System Microsoft Windows telah anda setting file sharing.

## Menjalankan Samba Network Neighbourhod

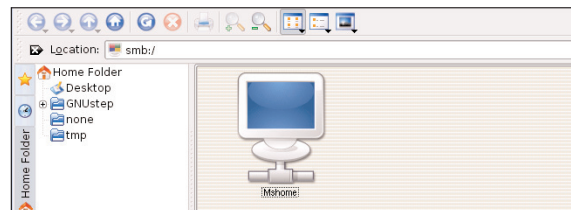
Setelah syarat-syarat yang disebutkan di atas telah terpenuhi, saatnya mencoba menjalankan Samba Network Neighbourhood.

Aktifkan modul Samba Network Neighbourhood.  
**Pacer>Linux>Utilities>Samba Network Neighbourhood.**



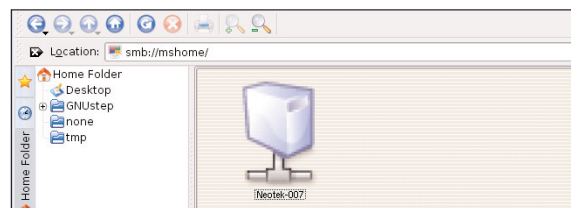
Gambar 1. Mengaktifkan Samba Network Neighbourhood

Memilih jaringan Windows File Sharing, Defaultnya jaringan file sharing di Microsoft Windows ada **Mshome**, tetapi itu bisa saja berubah tergantung kepada konfigurasi yang telah anda lakukan terhadap jaringan.



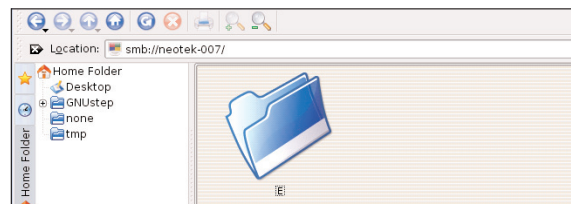
Gambar 2. Mshome

Memilih komputer yang telah ready file sharing-nya, ketika mencoba membuka file sharing di komputer lain yang menggunakan Microsoft Windows, yang terlihat nantinya adalah **nama komputer** tersebut.



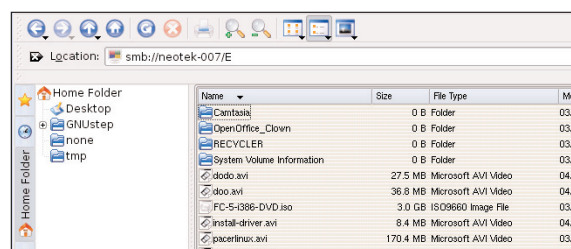
Gambar 3. Nama komputer

Memilih drive atau direktori, di PacerLinux baik drive atau direktori yang masuk dalam bagian setting file sharing, akan dikenal sebagai sebuah direktori oleh PacerLinux.

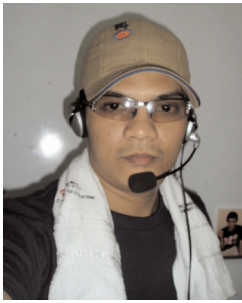


Gambar 4. Mengakses drive atau direktori

Selanjutnya adalah mengakses isi drive atau direktori.



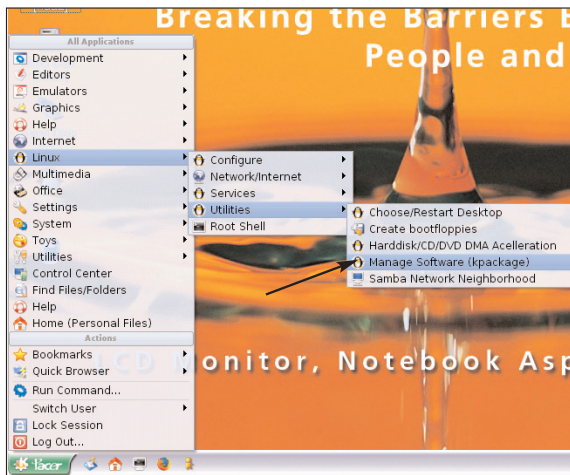
Gambar 5. Mengakses isi drive atau direktori



# PACERLINUX KPackage

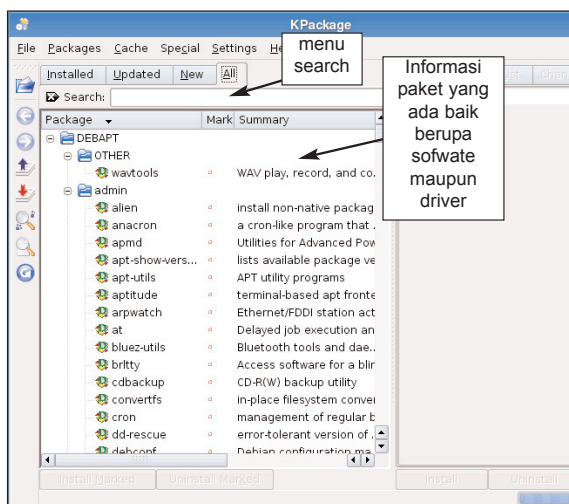
**Open Source Movement 2006** yang diusung oleh APKOMINDO dan didukung oleh PAZIA (distributor ACER di Indonesia untuk Aspire, Ferrari, dan LCD Monitor) meluncurkan distro baru PacerLinux. **MA Rody Candra** (support@pacerlinux.com) membahas seputar penggunaan PacerLinux.

**P**ADA SAAT MENJALANKAN PACERLINUX BAIK LIVE-CD maupun yang telah terinstalasi ke dalam harddisk, semua aplikasi baik berupa software maupun driver yang dipaketkan di dalamnya, dapat dilihat menggunakan fasilitas KPackage. **Pacer>Linux>Utilities>Manage Software (KPackage)**



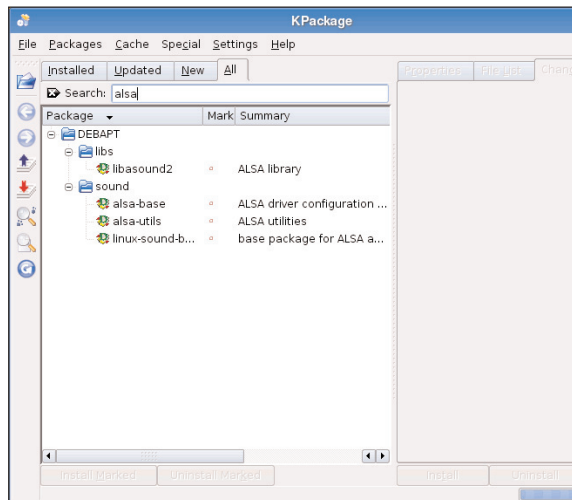
Gambar 1. Mengaktifkan KPackage

Setelah KPackage diaktifkan, akan muncul window dari KPackage itu sendiri yang berisi informasi yang berkaitan dengan aplikasi-aplikasi yang terdapat di dalam PacerLinux yang telah terinstalasi.



Gambar 2. KPackage

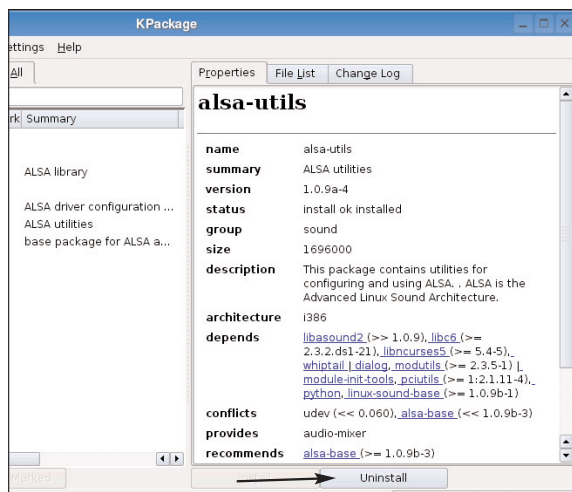
Banyak aplikasi yang dipaketkan ke dalam PacerLinux, tetapi anda dapat melakukan pencarian terhadap paket yang ada dengan memanfaatkan menu search.



Gambar 3. Memanfaatkan menu search di KPackage

## Uninstall

Jika dirasakan ada aplikasi yang tidak diperlukan oleh anda di dalam PacerLinux, anda dapat membuangnya (uninstall).



Gambar 4. Berhati-hati melakukan uninstall paket

*Note: Berhati-hati dengan urusan membuang isi paket, satu kesalahan bisa membuat PacerLinux anda tidak berjalan sebagaimana mestinya.*

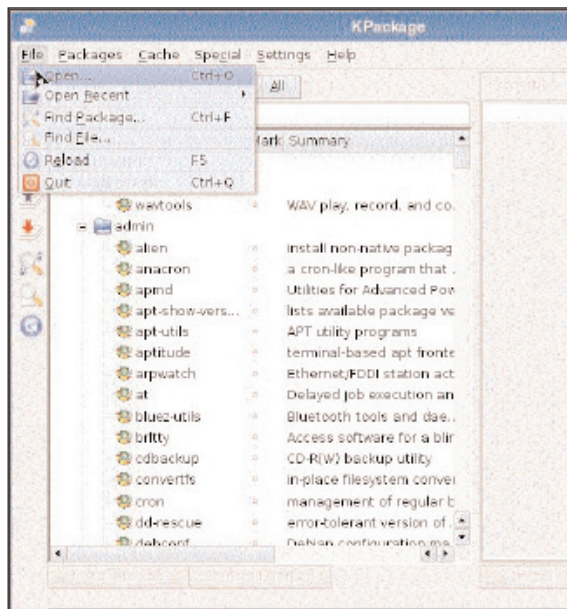


## Install

Ini merupakan kebalikan dari uninstall. Dalam hal ini yang anda lakukan adalah menambahkan software atau driver. Caranya adalah sebagai berikut:

**Aktifkan KPackage**, caranya lihat gambar 1.

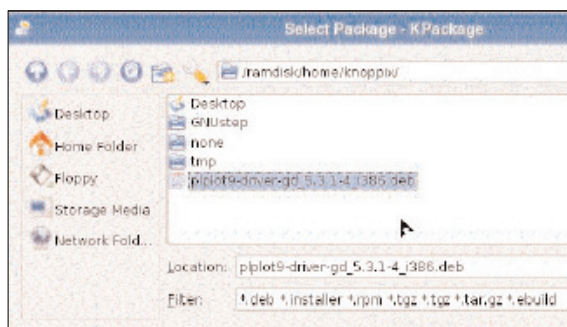
Open paket, **File>Open**



Gambar 5. Open file

**Pilih paket** yang telah dipersiapkan sebelumnya, kemudian klik **OK**.

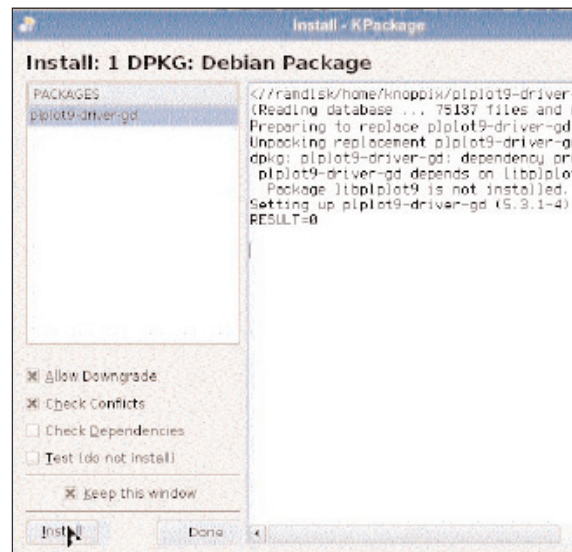
*Note: Paket yang dapat ditambahkan atau di-install adalah file dengan ekstensi **\*.deb** dan **\*.rpm***



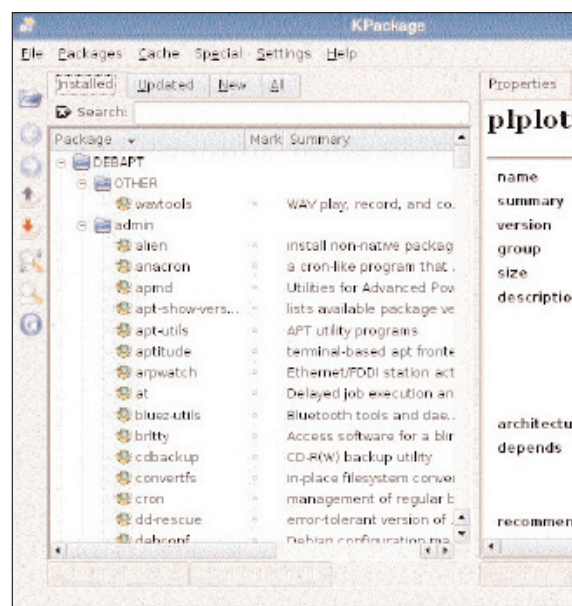
Gambar 6. pilih file

Beri tanda checklist pada opsi **Allow Downgrade**, **Check Conflicts**, dan **Keep this window**. Kemudian klik tombol **Install** yang berada di pojok bawah kiri, perhatikan gambar 7.

*Note: Disarankan untuk tidak memberi tanda checklist pada opsi **Check Dependencies** dan **Test (do not install)**.*



Gambar 7. Proses install



Gambar 8. Hasil install



# E-BANKING Tidak hanya Internet

**Perkembangan IT** memberikan solusi masalah yang terjadi di dunia perbankan, tetapi solusi tersebut diiringi masalah-masalah baru yang seyogyanya membutuhkan perhatian kita bersama. **Andi Ismayadi** (fuzk3\_kendi@yahoo.com) membeberkan semuanya sebagai informasi.

**C** ANGGIH YA, GAJI BULANAN KINI DISETORKAN MELALUI jasa **E-Banking**, atau ingin melakukan transfer uang kepada seseorang juga dapat dilakukan melalui jasa E-banking. E-Banking, apa itu? Internet banking kah? Untuk mengetahui seluk beluknya mari ikuti ulasan berikut ini.

Awal mulanya bank merupakan sebuah badan usaha jasa simpan pinjam uang, ketika itu penyetoran maupun penarikan tunai harus dilakukan lewat Teller. Yang terjadi adalah antrian yang panjang dan tentu saja akan menghabiskan banyak waktu, hal ini menjadi masalah pelik jika setiap harinya lebih dari seribu transaksi dilakukan.

Berpikir dan berpikir untuk memecahkan permasalahan tersebut untuk mengefisienkan waktu dan tenaga, IT dilirik dan diharapkan dapat memberikan solusi jitu sebagai alat untuk mempercepat dan menghemat waktu dalam transaksi. Jadi, tidak lagi antrian yang panjang, **cash-on-delivery** servis, transfer uang yang memakan waktu, dan lainnya. Era Electronic Banking (E-Banking) pun muncul, hadirnya mesin **ATM** (Automatic Teller Machines) atau Anjungan Tunai Mandiri yang berperan sebagai Teller.

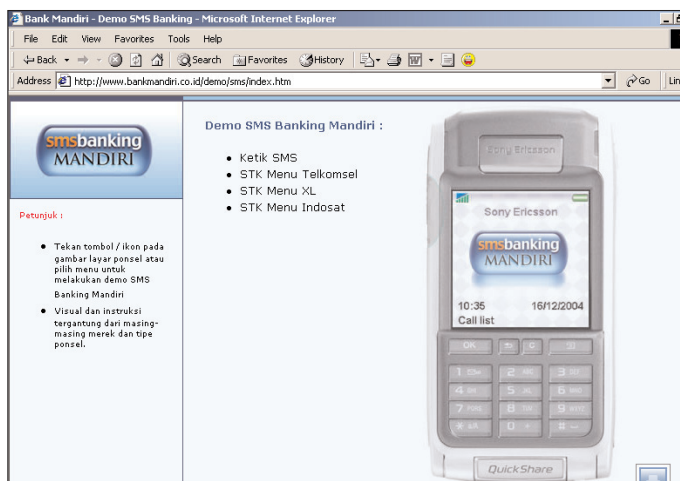
Kehadiran mesin ATM memberikan beberapa keuntungan seperti pelayanan **non-stop 24 jam**, transaksi penarikan tunai tidak perlu harus mengunjungi bank yang bersangkutan.

Apakah permasalahan sudah cukup teratasi? Kembali masalah antrian yang panjang tak terhindari dikarenakan pada awal kemunculannya jumlah mesin ini relatif sedikit dibandingkan sekarang, yang terjadi adalah adanya beberapa mesin yang **over-heated** sehingga jadi rusak (out of order). Masalah lainnya, kebutuhan transaksi perbankan tidak hanya sebatas penarikan tunai dan transfer, ada juga penyetoran tunai dan lain sebagainya. Pengadaan jumlah unit mesin ATM terus diperbanyak hingga hampir tiap sudut jalan sudah dihindangi mesin ATM. Tidak hanya pengadaan jumlah unitnya saja yang terus diusahakan, tetapi juga pengembangan teknologi mesin ATM itu sendiri hingga saat ini mesin ATM sudah dapat melakukan banyak bentuk transaksi, seperti penyetoran tunai, pembayaran tagihan telepon dan listrik, pembelian voucher isi ulang ponsel.

Implementasi IT pada E-Banking untuk mendukung dunia perbankan terus bergulir, hadir **SMS-Banking** atau **Mobil E-Banking**. Permasalahan tetap muncul ketika berada di daerah **blank spot** atau daerah yang tidak terjangkau layanan provider ponsel membuat anda tidak dapat mengakses SMS-banking, dengan begitu kerjasama antara pihak bank dengan pihak provider ponsel harus baik untuk mensukseskan E-Banking.



Gambar 1. Transaksi di mesin ATM



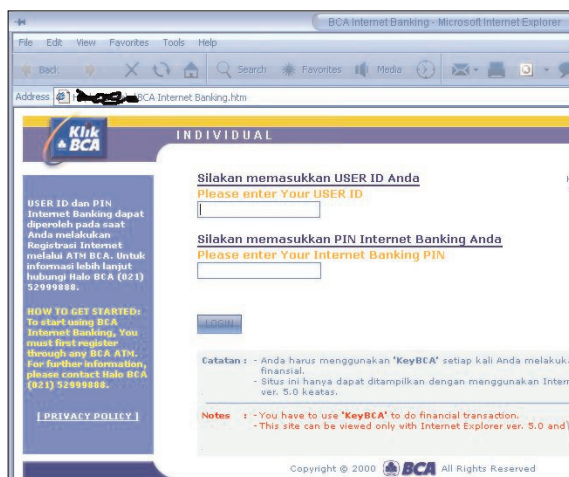
Gambar 2. SMS-Banking Mandiri

Implementasi IT pada E-Banking tetap terus melaju, hadir pelayanan Internet Banking, dimana anda bisa mengakses rekening Bank dari PC pribadi anda. Tentunya ada syarat untuk dapat melakukan akses ini, selain dituntut untuk



memiliki rekening pada Bank yang bersangkutan, koneksi internet menjadi keharusan. Dengan kombinasi syarat yang disebutkan tadi maka anda pun sudah melakukan transaksi mulai dari transfer antar rekening, beli voucher isi ulang ponsel, bayar listrik, telepon, dan lainnya.

Namun masalah masih tetap ada, diantaranya yaitu akses internet yang masih sukar didapat dan mahal, perbedaan bandwidth internet nasabah menjadikannya bermacam-macam keluhan. Jadi ketika mengakses fasilitas Internet Banking akan ada yang tidak dapat membuka halaman situsnya atau memakan waktu yang lama ketika mengakses rekening Internet Banking-nya. Masalah lainnya yaitu mengenai keamanan informasi nasabah, hal ini harus menjadi menjadi prioritas utama bank-bank yang memberikan fasilitas Internet Banking karena tidak semua nasabah melek atau sadar akan keamanan bertransaksi. Memberikan penyuluhan kepada nasabah bila perlu sebaiknya dilakukan agar mengakses Internet Banking melalui PC pribadi, penggunaan **Second Password**, **Randomize Password**, dan penggunaan fasilitas **Secure Socket Layer**.



Gambar 3. Internet Banking BCA

Dari ketiga jenis E-Banking yang telah dipaparkan, yang paling sering dilakukan nasabah adalah tarik tunai di mesin ATM, mungkin jenis lainnya segera merebak, dan adanya teknologi baru yang membuat nasabah lebih aman, nyaman dan efisien dalam bertransaksi.

### Sejarah E-Banking di Asia Tenggara

Implementasi E-Banking di Asia ternyata kurang begitu pesat, berikut perkembangan E-Banking di Asia.

- **Filipina**

Pada awal tahun 1980-an, **Citibank**, **Banks of The Philippine Islands (BPI)** [www.bpi.com.ph](http://www.bpi.com.ph), **Philippines National Bank**, dan bank-bank besar lainnya mempepori berdirinya teknologi E-Banking di negara kepulauan ini. Dan pada bulan Januari tahun 2000 BPI meluncurkan produk jasa terbarunya yaitu **BPI Express Online** dimana merupakan Internet Banking pertama dan nasabah bisa melakukan pembayaran, transaksi, kartu kredit dan lainnya.

- **Singapura**

Di Singapura sendiri internet banking pun mulai berkembang pada tahun 2001, dimana lebih dari 28% pengguna internetnya mengunjungi situs-situs

E-Banking (survei NetValue). Namun pada bulan Maret sampai Mei di tahun yang sama, waktu yang dihabiskan untuk mengunjungi situs tersebut menurun sekitar 4 menit, dikarenakan kebanyakan nasabah hanya melakukan transfer antar bank saja. Dengan banyaknya situs-situs E-Banking tersebut, dapat dipastikan hampir semua bank di negara ini memiliki internet dan teknologi IT yang cukup maju dan mereka menawarkan produk jasanya di situs-situs tersebut. Dan bank-bank ini mulai mengganti haluanannya dari retail-banking ke **SME** dan **Corporate Banking Products and Services**.

- **Malaysia**

Di Negara tetangga yang selalu ribut ini pun memakai teknologi IT untuk membangun jaringan E-Banking-nya. Dimana pada awal tahun 1981 ATM mulai muncul di negara ini, dan diteruskan dengan pengenalan E-Banking pada awal tahun 1990. Dan pada bulan Juni 2000, Malaysian Bank mengizinkan bank-bank komersial di negara tersebut untuk memakai teknologi Internet Banking, dan dengan ini pula **MayBank** ([www.maybank2u.com.my](http://www.maybank2u.com.my)) memulai membuat Internet Banking pertama di negeri jiran tersebut tepatnya pada tanggal 15 Juni 2000. Sistem internet banking yang dibuat MayBank mengimplementasikan **enkripsi 128-bit** untuk mengamankan transaksi perbankannya. Dan teknologi Internet Banking juga diterapkan bank-bank besar lainnya.

- **Indonesia**

Di negara kita tercinta ini, E-Banking muncul pada awal tahun 1981-1982 dimana **Bank Niaga** menerapkan jaringan online antar cabangnya. Lalu pada tahun 1987 Bank Niaga mengklaim dirinya sebagai pionir dalam penerapan teknologi ATM. Dan kini lebih dari 70 ribu ATM tersebar di seluruh Indonesia, disusul dengan perkembangan teknologi E-Banking lainnya seperti SMS-banking dan Internet Banking.

### Keuntungan E-Banking

Diantara sekian banyak fasilitas dan jenis yang ditawarkan E-Banking, yang menjadi prioritas dan andalannya adalah untuk melayani nasabah agar lebih efisien dan nyaman. Diantaranya ada beberapa keuntungan yang bisa didapat, antara lain:

- **EMail** yang digunakan nasabah memberikan keuntungan dalam berkomunikasi dan berkenalan dengan IT. Dan menambah kedekatan antar sesama nasabah, nasabah dengan bank, dan bank dengan bank lainnya.
- **Jasa dan informasi** selalu update secara real-time dan Online, sehingga dengan sekali klik maka nasabah bisa mengetahui jumlah saldo, jadi tidak lagi menunggu beberapa hari untuk mengetahui daftar transaksi dan jumlah saldonya. Dan daftar transaksi lainnya. Dan informasi dari bank dengan berita produk-produk dan jasa barunya.
- **Penerapan IT** dengan sistem perbankan menjadikannya sebuah alat yang sangat kuat dalam mengatur finansial, manajemen database, dan perhitungan transaksi tiap harinya dengan akurat dan selalu terjaga 24 jam.
- **Cash online** dapat dilakukan oleh nasabah dengan Internet Banking, misal anda ingin membeli sebuah iPod dalam sebuah webshop, namun anda tidak ingin pergi dan hanya ingin menunggu barang tersebut diantar kepada anda. Maka dengan Internet Banking,



## NeoTekno

pembayaran secara online dapat terjadi, ini juga harus didukung dengan fasilitas pembayaran yang ditawarkan webshop tersebut. Atau juga ingin **check and re-check** atau membayar uang kuliah secara online.

- **flexibilitas** yang ditawarkan Internet Banking disediakan kepada nasabah, yang dapat memungkinkan anda melakukan transaksi perbankan dimana pun anda berada. Di seluruh bagian Indonesia Raya ini ataupun di belahan dunia manapun, anda dapat memonitor keuangan anda sendiri.

E-Banking pun menjadi **jamur** baru dalam perkembangan IT di dunia, khususnya **Asia**. Namun teknologi ini belum mencapai sempurna karena kurangnya pendekatan yang dilakukan oleh bank-bank kepada calon nasabah untuk menggunakan jasa E-Banking, dan juga infrastruktur dan regulasi dari negara bersangkutan yang membatasi akses kepada khalayak umum.

*Lalu apakah E-Banking ini akan subur nantinya ataukah akan seperti ini-ini saja? Dan apa yang akan dilakukan pihak perbankan ini untuk menyuburkannya?*

Semua itu bisa berhasil apabila ada kerja sama antara, bank dengan nasabah, bank dengan pemerintah, dan bank dengan bank.

### Seputar E-Banking

**S**EDIA KALANYA BAHASAN MENGENAI E-BANKING dibahas pada 2 edisi yang lalu, tetapi baru pada edisi kali ini dapat diterbitkan. Untuk itu redaksi NeoTek mohon maaf kepada pembaca setia NeoTek.

Apa dan bagaimana itu E-Banking dibahas pada edisi ini, tetapi memang belum dapat menuntaskan dahaga ingin tahu pembaca NeoTek, tetapi setidaknya sudah dapat mengobatnya sedikit.

Perkembangan teknologi internet yang kian waktu makin melaju terus, menepis ramalan orang-orang yang pernah merasa pesimis dengan kehadiran internet dan mengatakn internet tiak akan berumur panjang.

Perkembangan internet yang maju tersebut dapat kita rasakan manfaatnya, contohnya yang paling dekat ada Email. Berkirim-kirim surat dengan sahabat, saudara, rekan bisnis, dan lain sebagainya dilakukan dengan mudah dan cepat berkat Email.

Dunia E sungguh memberikan keajaiban yang memungkinkan. Ada E-Government, E-Store, E-Book, dan lain sebagainya hingga E-Banking yang diulas dan anda baca sekarang ini.

Hampir seluruh badan usaha keuangan atau Bank di dunia, berlomba-lomba memberikan pelayanan terbaik untuk menyerap customer-customer baru maupun untuk memanjakan customer lama. Untuk melakukan berbagai transaksi keuangan tidak lagi perlu mendatangi Bank, semuanya kini dapat dilakukan melalui internet. Termasuk perbankan di Indonesia.

Tetapi kesadaran dan kepedulian akan keamanan atau dikenal sebagai Security Awareness tetap menjadi hal yang tidak boleh dilupakan.

**B** AGAIMANA KALAU ANDA INGIN MELAKUKAN TRANSFER sejumlah uang kepada kerabat hanya dengan menggunakan PC yang terhubung ke internet.

Dan ingin juga punya rekening bank di luar negeri tanpa harus beranjak dari depan komputer anda. Semua itu bisa dilakukan, anda hanya melakukan klik klik dan klik maka semua itu beres. Namun apa saja bank-bank yang ditawarkan bank online tersebut. Ikut lebih lanjut dalam artikel ini.

Perkembangan E-Banking di dunia sangat berkembang, dan ini membuka prospek baru dalam dunia perbankan, dan juga menguntungkan para nasabah. Internet banking pun lahir seiring perkembangan IT dan E-Banking ini, segala bentuk transaksi dengan media internet ini bisa dilakukan. Ada beberapa bank-bank atau pun lembaga keuangan bukan bank yang sudah terkenal di dunia dan maupun lokal.

#### • BCA

Bank yang sudah ternama dalam perbankan ini memiliki Internet Banking pertama di Indonesia, dengan KlikBCA anda bisa melakukan transaksi perbankan di internet dari rumah maupun dimana saja. Anda cukup membuka browser dan memasukkan alamat KlikBCA (<http://www.klikbca.com>) dan jangan salah memasukan alamat situs tersebut, karena KlikBCA pernah menjadi korban salah ketik, dimana ada seseorang yang membuat situs bayangan KlikBCA dengan URL [www.klikbca.com](http://www.klikbca.com) dimana situs ini telah menjaring data-data nasabah yang menjadi pengguna KlikBCA.



Gambar 1. KeyBCA

Segala jenis transaksi dapat anda lakukan di internet banking ini, kecuali tarik tunai. Kemudahan-kemudahan yang ditawarkan BCA dalam fasilitas E-



# E-BANKING Produk dan Jasa

**Perkembangan IT** memberikan solusi masalah yang terjadi di dunia perbankan, tetapi solusi tersebut diiringi masalah-masalah baru yang seyogyanya membutuhkan perhatian kita bersama. **Andi Ismayadi** (fuzk3\_kendi@yahoo.com) membeberkan semuanya sebagai informasi.

Bankingnya ini antara lain:

1. Pembelian (pulsa isi ulang, saham, tiket).
2. Pembayaran (kartu kredit, internet, telepon, handphone, pager, pendidikan, dan lain-lain).
3. Transfer Dana (transfer ke rekening BCA).
4. Informasi rekening (Informasi saldo, mutasi rekening, tagihan BCA Card).
5. Transaksi histori.
6. Administrasi (ganti PIN, ubah bahasa, ganti alamat email, hapus daftar pembayaran, hapus daftar transfer, registrasi KeyBCA, tambah koneksi KeyBCA, hapus koneksi KeyBCA, aktivasi KeyBCA, registrasi informasi BCA Card, hapus informasi BCA Card).

Untuk menjadi user (pengguna) KlikBCA, anda haruslah seorang nasabah BCA, dan menyerahkan tanda diri. Dalam pegamanan data dari Internet Banking ini BCA telah membuat suatu sistem pengamanan yang baik, dimana mereka menerapkan sistem enkripsi 128-bit, dengan begitu jaringan informasinya aman dari gangguan para Sniffer, dan juga mereka menggunakan Secure Socket Layer (SSL), selain itu para nasabah diwajibkan untuk memakai produk KeyBCA. KeyBCA adalah sebuah alat yang dapat menghasilkan pin acak yang berguna sebagai Second Password. Dengan KeyBCA juga data-data nasabah lebih aman dikarenakan ketika nasabah login ke [www.klikbca.com](http://www.klikbca.com) lalu ketika ingin melakukan transaksi maka nasabah wajib memasukkan password hasil generate acak dari KeyBCA tersebut, tanpa password acak ini transaksi yang disediakan KlikBCA tidak dapat dilakukan. Jadinya apabila data login anda dicuri orang, maka setidaknya uang anda masih aman tersimpan, karena tanpa password KeyBCA tersebut orang lain yang memiliki data login anda tidak bisa melakukan transaksi, baik itu transfer uang ataupun membeli pulsa ponsel.

BCA pun memiliki banyak ATM yang tersebar di seluruh Indonesia untuk memudahkan para nasabahnya untuk bertransaksi, dan BCA juga bekerja sama dengan bank-bank lainnya dalam teknologi ATM ini.

Selain dua produk diatas BCA, juga memiliki Kartu Passport BCA, yang berfungsi banyak atau multi-fungsi, dengan kartu ini anda bisa tarik tunai di ATM dan bisa menjadi kartu Debit BCA dimana berfungsi mirip dengan kartu kredit, bedanya deduksi pembayaran langsung diambil dari saldo anda. Jadi ketika anda berbelanja cukup membawa kartu BCA ini, anda sudah bisa melakukan berbagai macam transaksi, belanja, tarik tunai dan lainnya.

Teknologi SMS-banking pun dimiliki bank ini, dengan

nama produk m-BCA anda bisa melakukan transaksi seperti halnya dalam KlikBCA dengan media ponsel.

## • LippoBank

LippoBank juga memakai teknologi E-Banking dalam memperluas jaringan dan melayani nasabahnya, Internet Banking juga didirikan, namun tak seperti BCA, LippoBank Internet Banking ([www.lippobank.co.id](http://www.lippobank.co.id)) tidak terlalu bagus dari segi design. Sepertinya LippoBank kurang mengandalkan Internet Banking-nya. ATM menjadi andalan dalam jasa perbankannya, dan juga Lippo Credit Card.

## • Bank Mandiri

Sama Seperti KlikBCA, Internet Banking Mandiri ([www.bankmandiri.co.id](http://www.bankmandiri.co.id)) juga memiliki alat seperti KeyBCA, dengan nama produknya TOKEN PIN MANDIRI merupakan pengamanan dari sisi nasabah ketika melakukan login untuk bertransaksi di Internet Banking tersebut.



Gambar 2. Token PIN Mandiri

Jasa yang dilayani dalam Internet Banking Mandiri antara lain adalah:

1. Transfer antar rekening Bank Mandiri/Bank Domestik.
2. Transfer terjadwal.
3. Pembayaran tagihan: telkom, ponsel (GSM/CDMA), PLN, tiket Garuda Indonesia, Indosatnet, kartu kredit Mandiri Visa, Kompas dan XL Dealer.
4. Pembelian isi ulang pulsa (GSM dan CDMA).
5. Informasi rekening dan kartu kredit: tabungan, giro, deposito, pinjaman, kartu kredit.

## NeoTekno

6. Informasi nilai tukar valas dan suku bunga.
7. Pembukaan dan penempatan deposito.
8. Fasilitas layanan : status cek, notifikasi SMS.
9. Pendaftaran rekening tujuan SMS Banking Mandiri dan Call Mandiri.
10. Transaksi Perbankan lainnya.

Dari sisi pengamanan website, Mandiri sudah mengimplementasi *SSL 128-bit encryption, automatic LogOut* apabila dalam 10 menit tidak ada aktivitas dalam website tersebut dan apabila nasabah lupa untuk LogOut, *Firewall* juga mendukung web ini. Dan juga disediakan halaman khusus tips Internet Banking untuk para nasabah dalam melakukan transaksi yang aman.



Gambar 3. My Security Mandiri

SMS-Banking Mandiri juga menjadi andalan dalam E-Bankingnya, dengan fitur yang sama dengan Internet Banking Mandiri menjadikan SMS-Banking Mandiri pun diminati karena hampir semua nasabah Mandiri mempunyai ponsel.

Selain itu ATM mandiri juga tampil sama dengan banyaknya mesin ATM yang tersebar di seluruh nusantara ini.

### • Bank Permata

Tidak seperti BCA dan Mandiri, Permata Bank tidak melengkapi nasabahnya dengan alat sekuritas tambahan seperti Token PIN Mandiri ataupun KeyBCA. Di situs Permata Bank pun cukup menarik karena design yang pas, nasabah pun bisa melakukan transaksi internet bankingnya dengan produknya PermataNet di situs ini <https://www.PermataNet.com>. Selain juga dengan kartu ATM-nya.

### Online Banking International

Ada banyak bank online atau internet banking yang terdapat dalam jagat maya internet, dari berpuluh-puluh banyaknya yang paling terkenal antara lain **Paypal**, **E-gold**, **NetBullion**, **MoneyBrooker**, **Pecunix Cash**, **Qchex**, dan lainnya.

Dari sekian banyak Internet Banking dari bank ataupun lembaga keuangan bukan bank, hanya beberapa yang hidup dan lainnya mati terlindas yang lainnya. Matinya jasa Internet Banking disebabkan karena kurangnya kepercayaan nasabah akan bank itu, dikarenakan data nasabah yang mudah dicuri dan digunakan untuk keperluan yang

tidak sah. Situs Internet Banking-nya mudah ditiru dan dibuat *scam/phishing site*.

### Paypal

Paypal ([www.paypal.com](http://www.paypal.com)) merupakan sebuah lembaga keuangan bukan bank yang mempunyai jasa layanan Internet Banking. Paypal pun sampai sekarang masih hidup dikarenakan keamanannya yang ketat, dimana ada berlapis-lapis otoritas yang diterapkan kepada nasabahnya ketika melakukan transaksi. Dan tiap bulannya secara reguler Paypal melakukan *maintenance* terhadap sistemnya.

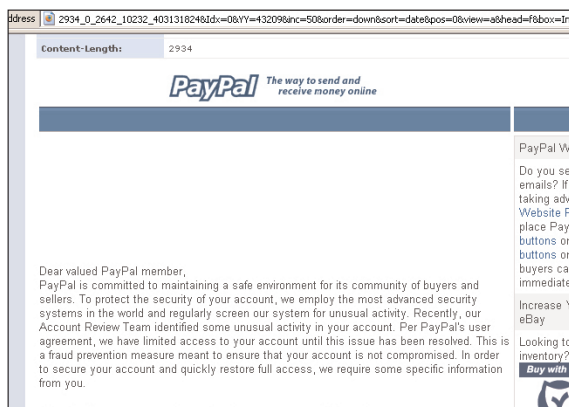
Dengan lebih dari 50 juta pelanggannya, Paypal menjadi **top leader** dalam **Online Payment** di dunia perbankan khususnya E-Banking. Cara kerja Paypal cukup simple, anda tinggal mendaftarkan diri anda di websitenya, lalu mengisi form dan menunggu konfirmasi. Anda bisa memasukkan nomor kartu kredit ataupun rekening bank yang akan di pakai oleh Paypal dalam melakukan deduksi pembayaran. Namun karena reputasi negara kita di dunia **Cyber Fraud** yang terkenal, maka bank di Indonesia tidak bisa dimasukan ke dalam Paypal, namun negara tetangga kita Singapura bisa dimasukan ke dalam rekening Paypal anda. Setelah itu, ketika anda telah terkonfirmasi maka, ketika anda melakukan pembayaran yang anda lakukan tidak perlu mengisikan lagi nomor pelanggan, nomor kartu kredit *seller*, ataupun nomor rekening *seller* tersebut. Melainkan anda hanya mengisi alamat E-Mail dari *seller* anda tersebut.

Begitu mudah dan aman, ini yang ditawarkan oleh Paypal untuk menjaga reputasinya dan untuk menambah nasabahnya. Sistem keamanannya yang dipakai antara lain dengan menggunakan *SSL 128-bit Encryption* dimana susahnyanya kemungkinan transaksi anda disadap orang lain atau di *sniff*, lalu dengan adanya *IP address match* dengan ini, IP address yang login pertama kali akan dicocokkan dengan IP address yang melakukan login kedua kali dalam beberapa jam, apabila IP addressnya ternyata tidak cocok, maka orang yang melakukan login kedua kalinya akan dihadapkan beberapa pertanyaan yang dikenal dengan nama *Security Measurement*, antara lain nomor kartu kredit beserta tanggal expire-nya atau nomor rekening bank. Apabila pertanyaan ini tidak dijawab atau salah, maka orang yang melakukan login ini akan langsung keluar dari halaman login. Dan Paypal akan segera mengirimkan E-Mail pemberitahuan kepada pemilik rekening ini, bahwa ada seseorang yang berusaha login pada jam sekian dengan IP address sekian, jadi si pemilik sah akan tahu apa itu dia yang melakukan atau orang lain yang mengetahui user login-nya. Nasabah tersebut diharuskan mengganti password-nya supaya tidak lagi digunakan oleh orang yang tidak sah.

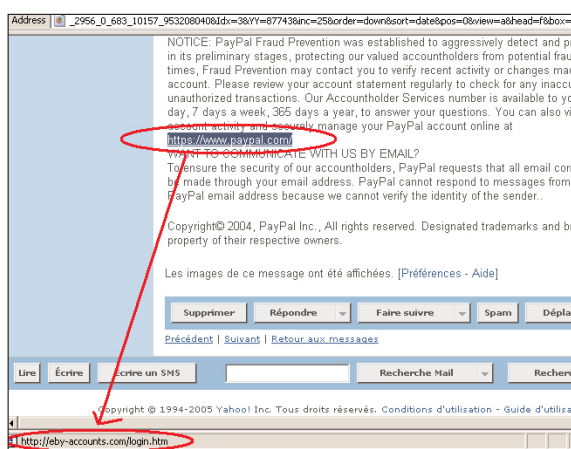
Beberapa masalah keamanan mengincar para nasabah Paypal, ini dikarenakan memang Paypal sudah di incar sejak awal mula kemunculannya. *Scam/phishing mail* yang banyak diterima oleh para nasabah Paypal pun memakan korban, tidak sedikit nasabah yang terjebak akan e-mail *phishing/scam* yang memberitahukan berbagai macam informasi tentang rekening si nasabah yang intinya adalah agar pasha nasabah tersebut melakukan registrasi ulang di web *scam/phishing* yang mirip sekali dengan website aslinya [www.paypal.com](http://www.paypal.com)

Untuk itu Paypal menghimbau kepada para nasabahnya agar memperhatikan alamat URL paypal di browser masing-masing.





Gambar 4. Email phishing



Gambar 5. Scam Paypal

Kebijakan Paypal pun wajib di patuhi para nasabah agar rekeningnya aman dari penggunaan tidak sah, antara lain password yang wajib 8 karakter dan kebijakan lainnya. Karena Paypal tidak menanggung apabila rekening nasabah dicuri dari sisi nasabah, Paypal hanya mengamankan sistemnya di dalam terhadap serangan-serangan luar yang ingin mengambil database Paypal.

Selain itu kemudahan yang ditawarkan Paypal adalah kemudahan mencari toko *E-shop* dimana banyak sekali yang menggunakan Paypal sebagai salah satu alat pembayarannya, dan terkadang ada diskon yang ditawarkan apabila membayar melalui Paypal.

### E-Gold

Selain Paypal, ada juga sebuah lembaga keuangan bukan bank yang bisa melakukan transaksi melalui internet. Apabila Paypal tadi tidak ataupun susah digunakan untuk sebagian orang Indonesia, maka E-gold ([www.e-gold.com](http://www.e-gold.com)) tidak susah, karena sifatnya *universal* dan mudah menjadikannya *survive* dalam bisnis E-Banking ini.

Satuan mata uang dari seluruh dunia ada di dalam sistem perbankan E-gold. Dalam E-gold sendiri terdiri dari beberapa mata uang khusus, antara lain *metal*, *gold*, *palladium*, *platinum*, dan lainnya. E-gold sendiri sudah bekerja sama dengan beberapa bank di dunia dan di Indonesia, BCA sebagai salah satu bank yang dipakai untuk melakukan pembayaran dan pembelian mata uang E-gold. Dengan ATM anda bisa membeli mata uang E-gold, ataupun dalam

mata uang lainnya seperti dollar, poundsterling ataupun euro.

### GreatAchiever

Lalu kalau kita bisa beli mata uang tersebut, dimana kita bisa mencairkannya? [www.greatachiever.com](http://www.greatachiever.com) salah satu lembaga keuangan bukan bank di Internet Banking bisa mencairkannya langsung ke rekening BCA anda. Karena greatachiever sendiri adalah buatan anak negeri sendiri, di website ini anda dapat bertukar informasi ataupun menjual gold anda. Ada forum dimana anda dapat bertukar informasi tentang Internet Banking yang satu ini, bagaimana untuk menghasilkan gold, ataupun bertukar informasi tentang keamanan E-gold.

Web ini telah menjadi korban *scam/phishing* ketika muncul web [www.greatachiever.com](http://www.greatachiever.com) (tanpa huruf E setelah huruf I dan sebelum huruf V) namun sayangnya peringatan muncul telat, karena ketika web scam tersebut muncul, belum ada peringatan dari sang admin. Walaupun telat admin greatachiever.com pun segera meng-update halaman depan websitenya dengan menambah pengumuman tentang web scam/phishing tersebut. Belum ada laporan tentang siapa saja korban dibalik scam/phishing web ini. Masalah keamanan pun menjadi sarat utama di web ini, dimana terdapat tips dan trik untuk bermain-main E-gold.

E-gold juga menggunakan SSL dan beberapa keamanan lainnya seperti, *second password* berupa angka-angka dalam gambar secara acak, lalu password nasabah yang wajib 6 karakter dan juga harus memiliki kombinasi angka dengan huruf. Tidak hanya itu, apabila anda sudah login, maka anda akan diminta *AccentPin* yaitu konfirmasi 6 digit angka yang dikirim ke e-mail nasabahnya. Dan jika dalam 15 menit atau 3 kali salah, memasukkan angka tersebut, *accentpin*-pun akan dikirim ulang kembali. Autentifikasi serupa login diterapkan dalam setiap transaksi, ketika anda ingin melakukan transfer maka login ulang akan muncul kembali, dan bukti transfer tersebut masuk ke dalam *History Payment*.

Seperti BCA, greatachiever.com, paypal.com, e-gold.com pun menjadi sasaran scam/phishing website. Ini dikarenakan kemudahan E-gold dalam mengirim uang dan cepatnya pencairan uang dari uang maya ke uang asli. Ada beberapa toko jual beli barang yang melakukan scam dimana ketika nasabah membayar barang tersebut dengan E-gold maka *seller* (penjual) barang dari toko tersebut hanya menunggu sampai E-gold-nya banyak dan langsung cair ke rekeningnya. Lalu apa akibatnya bagi si *buyer* (pembeli), yang dihasilkan bukan berupa barang melainkan hanya tinggal gigit jari melihat E-gold-nya kosong.

Apapun kegiatannya E-Banking merupakan perkembangan IT terbaru dalam dunia E-Commerce, dilihat dari sisi positif dan menjamurnya *scam/phishing*, *cyber fraud* yang diakibatkan sisi negatifnya.

Kesadaran dari diri sendiri sebagai nasabah perlu di tingkatkan agar tidak menjadi korban *scam/phishing*. Dan dari perusahaan E-Banking perlu melakukan *maintenance* sistemnya secara berkala, *penetration test* dari dalam perlu juga dilakukan untuk mengukur dan mengontrol tingkat keamanan sistem perbankannya, update situs secara berkala, dan lain sebagainya merupakan langkah penting yang dilakukan, agar tidak terjadi hal-hal yang tidak diinginkan.

Dengan begitu semakin banyak calon nasabah yang mendaftar dan meningkatkan kredibilitas dan citra dari masing-masing perusahaan E-Banking tersebut.



# E-BANKING Seluk Beluk Paypal

**Perkembangan IT** memberikan solusi masalah yang terjadi di dunia perbankan, tetapi solusi tersebut diiringi masalah-masalah baru yang seyogyanya membutuhkan perhatian kita bersama. **Andi Ismayadi** (fuzk3\_kendi@yahoo.com) membeberkan semuanya sebagai informasi.

**S**ETELAH KITA KETAHUI SEBELUMNYA TENTANG PAYPAL sebagai online payment dalam E-Banking. Paypal pun memiliki rahasia tersendiri yang kurang disadari oleh para nasabahnya, untuk itu akan dibahas rahasia apa saja yang dimilikinya. Sebelum itu ada beberapa informasi umum yang akan dibedah juga.

Paypal memungkinkan nasabahnya untuk mengirim dan menerima uang dengan hanya identifikasi email yang terdaftar sebagai nasabah.

Contoh skenarionya sebagai berikut;

*Joni mempunyai rekening di Paypal dengan email identifikasi joni\_kemod@yahoo.com, lalu ia ingin mengirimkan sejumlah uang ke pacarnya di Inggris yang juga terdaftar di Paypal dengan email identifikasi pacarnya\_joni@yahoo.com.*

Maka dengan satu kali klik, sejumlah uang pun terkirim dan pacarnya Joni pun bisa langsung mengambilnya di bank lokal dimana rekeningnya berada dan telah didaftarkan ke Paypal.

Lalu apa hanya transfer saja yang dimiliki Paypal? Dan apa harus membuat/mendaftar sebagai nasabah Paypal dulu sebelum berkirim uang? Untuk jelasnya ikuti bahasan berikut.

## Paypal Registration

Kunjungi situs resmi Paypal di [www.paypal.com](http://www.paypal.com). Pada halaman pertama dari situs paypal, klik **Sign Up** dan pilih opsi **Personal Account**, pilih negara anda dan kemudian klik **Continue**.

Gambar 1. Mendaftar untuk rekening Paypal

Anda akan menemukan halaman formulir yang harus anda isi semua dengan ketentuan data-data pribadi, isilah

dengan benar dan jelas karena data-data tersebut akan di cek ulang oleh Paypal. Ketika memasukkan email dan password, sebaiknya bedakan dengan password email anda agar rekening anda nantinya tidak mudah untuk diakses oleh orang yang tidak bertanggung jawab. Masukkan nomor telepon dengan benar, fungsinya adalah anda bisa mengambil akses rekening anda apabila suatu hari nanti anda mengalami lupa password. Isi jawaban **Security Question** yang berguna untuk pertanyaan ulang ketika melakukan perubahan password atau mengambil password yang terlupa. Lalu pilih **No** dalam pilihan **you'd like this to be a Premier Rekening**. Pilih **Yes** jika anda setuju dengan **User Agreement**, lalu masukan karakter **security measurement** dan selesai.

Anda baru saja memiliki rekening Paypal. Tapi tunggu dulu, ini bukan berarti anda bisa melakukan transfer langsung, karena Paypal harus mengkonfirmasi rekening anda supaya sah menjadi alat pembayaran. Dan anda juga harus mengkonfirmasi nomor telepon, email, dan alamat anda.

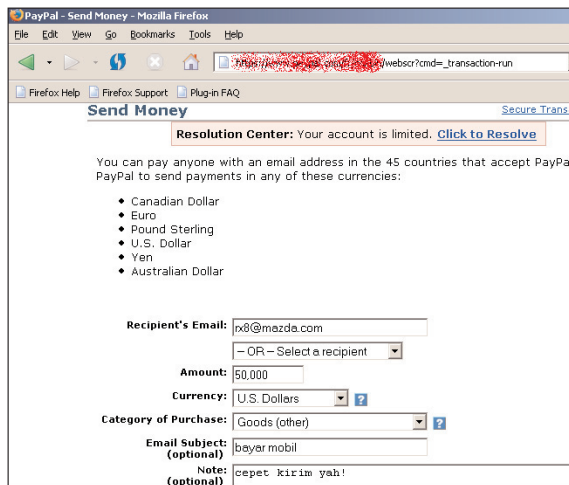
Status yang anda terima setelah mendaftar seperti di atas adalah **unverified** artinya anda belum disahkan oleh Paypal untuk melakukan transfer dan menikmati fitur lainnya. Untuk itu anda perlu menjadi **Verified** untuk bisa membuka semua fitur tersebut. Untuk Menjadi Verified maka anda diwajibkan memasukan bank rekening di tab **My Rekening - Profile** dan klik **Bank Rekenings**, lalu isi data-data formnya, untuk pengisian bank tersebut anda tidak bisa menggunakan rekening bank di Indonesia karena Paypal belum mempercayainya, beberapa bank yang bisa gunakan antara lain negara Inggris, Amerika, Singapura.

Setelah itu anda akan diminta untuk mengkonfirmasi rekening bank anda ke Paypal, dan sebagai bonusnya maka Paypal memberi anda sedikit uang sebagai rasa terima kasih telah mempercayai Paypal untuk menjadi alat pembayaran di dunia maya. Enak bukan membuka rekening gratis dan menerima sejumlah uang.

Setelah Verified maka anda bebas berbelanja sepuasnya, atau juga anda bisa memberikan limit agar tidak terbuang-buang, biasanya limit paling besar adalah **US\$2000**.

Dan untuk memonitor rekening Paypal anda, maka setiap kali transaksi akan ada history-nya (log) atau informasi tentang pembayaran atau penerimaan uang terakhir di halaman awal web member Paypal.

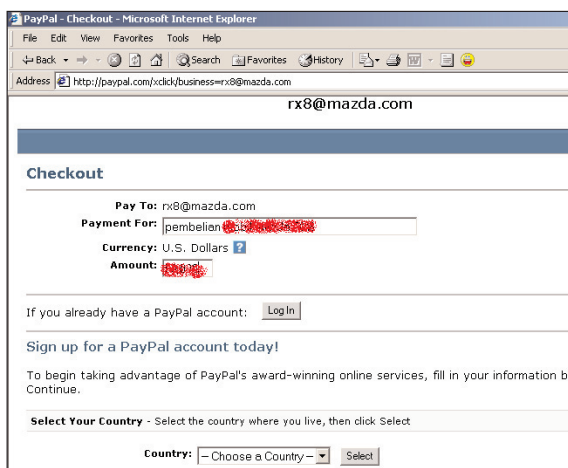
Untuk mengirim uang kepada teman atau kerabat bahkan **seller** anda tinggal memilih tab **Send Money**, isikan data-data tersebut sesuai dengan informasi yang anda peroleh tentang status pengiriman pembelian sebelumnya. Dan jangan sampai anda salah mengetikkan alamat email, karena untuk mengembalikan uang yang sudah dikirim sangat susah. Fitur pengiriman uang Paypal dapat menjadi alat pembayaran **seller ebay**, dan **webshop** yang menyediakan pembayaran lewat Paypal ini.



Gambar 2. Memanfaatkan fitur Send Money di Paypal

Fitur lain yang disediakan Paypal yaitu fitur **meminta uang** atau **request money**. Fitur ini dapat meminta seseorang yang telah terdaftar menjadi nasabah Paypal untuk mengirim uang kepada anda, tentunya dengan sebuah perjanjian terlebih dahulu sebelumnya. Mungkin untuk pembayaran uang kuliah anda meminta orang tua anda yang sedang berada di luar negeri dan keperluan lainnya.

Salah satu rahasia yang tidak semua orang tahu tentang Paypal adalah dimana anda tidak perlu mendaftar menjadi nasabah Paypal, karena anda bisa membayar orang dengan Paypal tanpa menjadi nasabah. Caranya adalah dengan membuka link Paypal berikut <http://Paypal.com/xclick/business=tujuan@pembayaran.com> dimana [tujuan@pembayaran.com](mailto:tujuan@pembayaran.com) adalah email seseorang yang sudah terdaftar sebagai **Paypal verified member**, dan anda ingin mengirim uang VIA Paypal kepadanya. Lalu ikuti pengisian form selanjutnya seperti ketika mendaftar pertama kali.



Gambar 3. Fitur pengiriman uang bukan sebagai member Paypal

Paypal sendiri juga menyediakan **search engine** untuk mencari toko-toko tertentu dengan kriteria para nasabahnya. Dengan mengetikkan [https://www.Paypal.com/us/cgi-bin/webscr?cmd=\\_shop-ext](https://www.Paypal.com/us/cgi-bin/webscr?cmd=_shop-ext) di browser maka, anda dapat mencari toko-toko dengan fasilitas pembayaran Paypal, dan anda tidak perlu mencari-cari di Google lagi.

## Trend Micro Press Release

Jakarta, Indonesia -20 April 2006 - Trend Micro Inc.

InterScan Web Security Appliance mewakili teknologi paling mutakhir yang dimiliki oleh perusahaan yang memimpin di bidang perangkat pengaman gateway, dan produk ini sekaligus memperkuat langkah pendekatan Trend Micro dalam usaha melindungi perusahaan-perusahaan dari spyware maupun ancaman lainnya. Perangkat ini bertindak sebagai lapis pertama perlindungan terhadap serangan spyware, grayware, virus, dan phishing. Perangkat ini juga menawarkan kemampuan unik yang dapat mengaktifkan secara otomatis proses pembersihan dengan bekerjasama dengan Trend Micro™ Damage Cleanup Services. Selain itu, perangkat ini juga mampu mendeteksi dan memblokir malware, menyaring URL, anti-phishing dan fitur-fitur lainnya untuk mencegah ancaman seperti spyware masuk ke dalam jaringan.

Secara keseluruhan, perangkat ini menambah keuntungan yang diberikan oleh "Strategi Perlindungan Perusahaan" atau Enterprise Protection Strategy (EPS) yang dimiliki oleh Trend Micro. Perangkat ini memberikan pilihan yang lebih baik dalam hal perlindungan gateway bagi organisasi bisnis, dengan memperkenalkan pilihan hardware yang mudah dioperasikan, InterScan, yang berbasis software pemenang penghargaan dari Trend Micro. Sebagai tambahan, InterScan Web Security Appliance dapat bekerjasama dengan produk keamanan Trend Micro lainnya, seperti Trend Micro™ Anti-Spyware Enterprise Edition™ dan OfficeScan™, sehingga memberikan solusi keamanan yang berlapis, fleksibel, dan dapat melindungi setiap aspek dalam sebuah jaringan bisnis - sejak gateway internet lalu web server hingga ke desktop komputer.

"InterScan™ Web Security Appliance sangat mudah dipasang dan dikonfigurasi," ujar Paul Kim, Manajer Infrastruktur Departemen IT untuk Coca Cola Korea Bottling Company, Ltd, salah satu perusahaan dunia yang telah menggunakannya. "Lebih lanjut, perangkat ini jauh lebih efektif daripada menggunakan keamanan desktop sendiri dengan perlindungan terpadu anti-spyware, antivirus, anti-phishing dan penyaringan URL di gateway internet. Peluncuran produk solusi keamanan Web terpadu dari Trend Micro ini memungkinkan kami lebih santai menghadapi ancaman malware maupun ancaman internet lainnya."

Kehadiran InterScan Web Security Appliance bertepatan dengan isu berkembangnya spyware dan ancaman lainnya yang menjadi tantangan bagi organisasi IT dan pengguna. Sebagai contoh, pada bulan Juli 2005 Trend Micro melakukan survey global terhadap perusahaan pengguna akhir, dan hasilnya menunjukkan 39% responden merasa bahwa IT seharusnya dapat melakukan lebih banyak hal untuk mencegah bertambahnya korban spyware dan phishing. Pada tahun yang sama, sebuah survey yang dilakukan oleh IDC mengungkap bahwa spyware digolongkan sebagai ancaman keamanan kedua yang paling ditakuti oleh perusahaan.

"InterScan Web Security Appliance dari Trend Micro ini memiliki kemampuan untuk mengatasi spyware seperti yang kami butuhkan" ujar Joe Fiorella, seorang analis keamanan informasi dari Reader's Digest di Amerika Serikat. "Perangkat ini telah terbukti efektif dalam mencegah paparan spyware, dan lebih khusus kami menyukai kemampuannya menyaring website dan memblokir beberapa tipe file."

"Kami yakin kami satu-satunya vendor yang dapat menghadang daur hidup lengkap spyware dengan pendekatan berlapis dalam jaringan perusahaan," ujar Max Cheng, Wakil Pemimpin Umum dan General Manager segmen Perusahaan Bisnis dari Trend Micro. "Pendekatan berlapis ini memungkinkan kami untuk mencegah, mendeteksi, memblokir dan membersihkan spyware, grayware, dan malware sebagai bagian dari solusi komprehensif untuk perusahaan-perusahaan besar. Perangkat ini memberikan amunisi tambahan bagi perusahaan - serta pilihan yang lebih baik - untuk melindungi investasi IT mereka dan para pengguna dari spyware dan ancaman berbahaya lainnya."





# E-BANKING E-Gold Lebih Jauh

**Perkembangan IT** memberikan solusi masalah yang terjadi di dunia perbankan, tetapi solusi tersebut diiringi masalah-masalah baru yang seyogyanya membutuhkan perhatian kita bersama. **Andi Ismayadi** (fuzk3\_kendi@yahoo.com) membeberkan semuanya sebagai informasi.

**O**NLINE PAYMENT YANG SATU INI MULAI DIGEMARI orang-orang di Indonesia, karena kemudahan dalam pendaftaran, gratis, dan bisa langsung cair. Dengan begitu anda bisa berinvestasi di perusahaan orang dengan bagi hasil melalui pembayaran E-gold. Apa saja tip dan triknya? Temui dalam ulasan berikut ini.

## E-Gold Registration

Sebelumnya, anda harus mendaftar terlebih dahulu, kunjungi situs resminya di [www.e-gold.com](http://www.e-gold.com). Pada halaman-nya cari dan klik link untuk pendaftaran, selanjutnya anda akan berhadapan dengan klausul perjanjian yang harus anda setujui. Kemudian isi form register, maka anda sudah menjadi member dari E-gold.

Gambar 1. Mendaftar untuk rekening E-gold

Tapi anda tidak akan mengetahui nomor rekening anda di E-gold.com, ketika anda telah di approve menjadi member dengan pengisian form registrasi, secara otomatis E-gold akan mengirimkan email pemberitahuan nomor rekening dan lainnya ke email anda yang telah diregistrasikan. Setelah mengetahui nomor rekening, maka anda dapat mengakses rekening anda di E-gold.

## Login Session

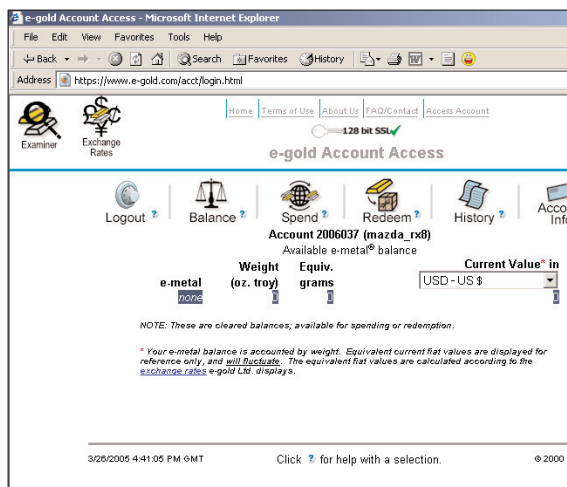
Login dengan memasukkan nomor rekening dan password dan juga **touring number** yaitu sebuah angka acak untuk menjadi **second password** anda. Ketika anda login dengan IP address yang berbeda dengan IP address ketika anda mendaftar, maka anda akan dihadapkan dengan PIN khusus sejumlah 6 digit yang dikirimkan ke email anda dan akan dikirim setiap 15 menit apabila anda belum juga memasukkannya atau anda salah memasukkannya.

Gambar 2. Konfirmasi nomor rekening E-gold

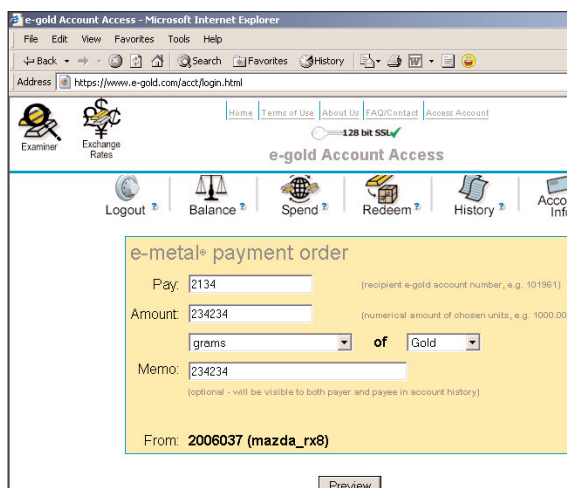
Gambar 3. AccSent PIN

PIN akan dikirimkan setelah anda masuk ke halaman **AccSent-PIN**, lalu masukan PIN tersebut ke **input box** yang terdapat di halaman AccSent PIN. Masuk ke halaman **Balance** untuk melihat saldo rekening anda. Untuk mengirim E-gold ke rekening teman ataupun siapa pun yang berkepentingan, klik saja link **Spend**. Untuk membeli atau menjual E-gold, sebaiknya anda menjualnya di web yang terpercaya yaitu **www.greatachiever.com**.

*Note: Jangan salah memasukkan URL atau anda akan menjadi korban scamming.*

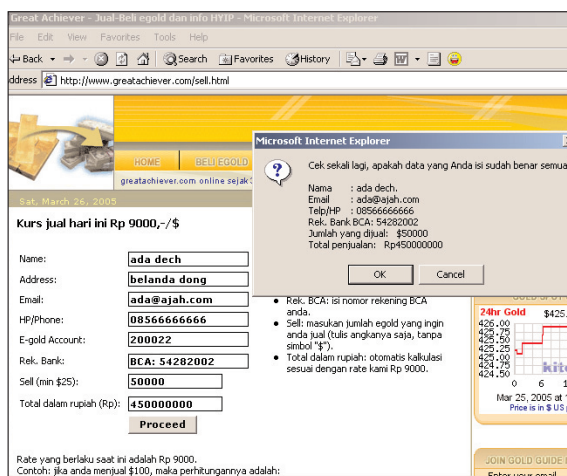


Gambar 4. Memeriksa saldo rekening di E-gold



Gambar 5. Fitur mengirim sejumlah E-gold

Semua harga akan ter-update seiring perkembangan perekonomian dunia, dan berpatokan kepada harga dollar. Dan Kalau anda ingin menjual E-gold atau dengan kata



Gambar 6. Fitur menjual sejumlah E-gold

lain mencairkan E-gold, maka klik **Sell E-gold**, dan seperti sebelumnya anda wajib mengisi data-data anda, mulai nama, sampai nomor rekening bank anda.

*Note: Sebaiknya ketika anda akan menjual E-gold, perhatikan terlebih dahulu keadaan mata uang dan nilai tukar yang tersedia, hindari penjualan ketika harga rendah. Akan lebih menguntungkan menjual ketika harga E-gold sedang tinggi. Ketika membeli pun belilah ketika harga E-gold sedang turun.*

## HYIP

Lalu apa untungnya dengan program online payment ini dengan E-gold? Banyak orang yang di dunia ini meraih keuntungan dengan bermain-main dengan E-gold, salah satu cara untuk mendapatkan keuntungan adalah dengan mengikuti program **HYIP** (High Yield Investment Programme), disini menanamkan modal dengan E-gold anda dan dalam beberapa waktu akan mendapat keuntungan sesuai kebijakan pengembang HYIP tersebut.

Selain itu anda juga dapat membeli barang-barang yang sedikit lebih murah di internet dengan pembayaran menggunakan E-gold.

*Note: Berhati-hati ketika mencari web HYIP ataupun toko karena banyak juga scammers yang melakukan penipuan melalui cara membuat web HYIP bohong-bohongan dan mengambil E-gold anda tanpa adanya pembayaran nantinya.*

Untuk menghindari web scam ini sebaiknya anda memperhatikan terlebih dahulu informasi yang ditawarkan. Biasanya HYIP asli memang lama dalam melakukan pembayaran keuntungan, berbeda dengan HYIP palsu yang menawarkan keuntungan besar dengan waktu yang singkat atau lebih cepat dibandingkan HYIP asli. Selain itu, sebaiknya anda juga melakukan pengecekan registrasi situs tersebut di <http://www.dnsstuff.com>, lihat nama pemiliknya, tanggal pendaftaran. Dan HYIP palsu biasanya tidak terlalu lama online dibandingkan yang asli.

## Download by Request

Mulai edisi Vol. VI - No. 3

**AMKM** (Anda Meminta Kami Men-download), rubrik yang menerima permintaan download software dari pembaca NeoTek, rubrik tersebut sempat terhenti karena suatu alasan.

Kini NeoTek kembali mengaktifkan rubrik AMKM dengan nama baru yaitu **Download by Request**.

Tetapi ada peraturan yang harus dipatuhi bagi anda yang ingin kembali memanfaatkan rubrik ini.

Peraturannya adalah sebagai berikut:

- Download dibatasi sebesar 50MB/orang
- Program/software yang diminta harus berupa:
  - Free software
  - Demo software
  - Trial software
  - Open Source software

Bagi yang tidak mengacu kepada peraturan yang disebutkan di atas, permintaan tidak akan dilayani.

Bagi yang berminat, silakan kirimkan informasi link program/software yang diminta ke email [support@neotek.co.id](mailto:support@neotek.co.id) dengan subject email **Download by request**.

NeoTek akan mengkonfirmasi melalui email bagi yang permintaan download by request dimuat.

Pastikan anda memanfaatkan kesempatan ini.



# E-BANKING Sisi Gelap & Pencegahan

**Perkembangan IT** memberikan solusi masalah yang terjadi di dunia perbankan, tetapi solusi tersebut diiringi masalah-masalah baru yang seyogyanya membutuhkan perhatian kita bersama. **Andi Ismayadi** (fuzk3\_kendi@yahoo.com) membeberkan semuanya sebagai informasi.

**M**EMANG MENARIK KEGIATAN TRANSFER UANG DI ALAM maya, selain mudah dan cepat, nasabah hanya melakukannya dari rumah saja. Internet banking jadi komoditas utama orang-orang yang mobile dan selalu ingin *up-to-date* dengan rekening banknya. Namun, tidak sedikit orang-orang yang stress, bahkan sampai bunuh diri akibat Internet Banking. Kenapa bisa begitu? Ini disebabkan ketika rekening bank tersebut dipakai untuk hal yang tidak-tidak, **cyber fraud** mendominasi dunia E-Banking khususnya Internet Banking.

Bagaimana ini bisa terjadi dan apa saja trik atau usaha yang dilakukan untuk mendapatkan pengguna rekening secara tidak sah? Akan anda temui dalam bahasan ini.

Bank membuat sistem dengan seketat-ketatnya, namun bocornya data tetap terjadi. Ternyata survei yang dilakukan oleh **ebankingsecurity.com** menyebutkan bahwa sistem yang canggih dari bank merupakan alat cuci tangan bank tersebut atas kebocoran data nasabah, dan ternyata rantai yang sangat lemah terdapat pada sisi nasabah, karena nasabah sudah diberikan gambaran bahwa Internet Banking yang mereka pakai sangat canggih dan aman, sehingga mereka tidak sadar bahwa dengan begitu ancaman pun pindah ke sisi yang lemah yaitu sisi nasabah.

Tanpa kesadaran akan keamanan data, maka nasabah tidak perlu khawatir, tetapi dengan begitu nasabah selalu ada juga nasabah yang lalai dengan sembarangan mengakses Internet Banking dari PC manapun. Sehingga ketika suatu kali data login tersebut terekam oleh Keylogger, maka bank sekalipun tidak dapat berbuat apa-apa. Apabila nasabah menuntut maka bank lepas tangan karena kebocoran data tersebut merupakan kesalahan itu nasabah sendiri.

Untuk meningkatkan kewaspadaan akan pencurian data login khususnya Internet Banking, ada baiknya anda mengetahui beberapa cara dan ancaman yang bisa **merebut** rekening Internet Banking anda. Dan informasi ini hanya dijadikan acuan untuk sarana menambah pengetahuan dan tidak dianjurkan untuk disalah gunakan, seperti mencuri rekening orang lain. Oleh sebab itu apapun yang ditimbulkan artikel ini, penulis tidak bertanggung jawab.

Sekali lagi penulis tegaskan, tujuan artikel ini hanya sebagai informasi untuk memberi pengetahuan akan bahaya atau ancaman yang mengintai para pengguna Internet Banking, dan dengan ini diharapkan *Security Awareness* dapat diterapkan, dengan begitu kasus kebocoran data dan **Cyber Fraud** dapat ditekan.

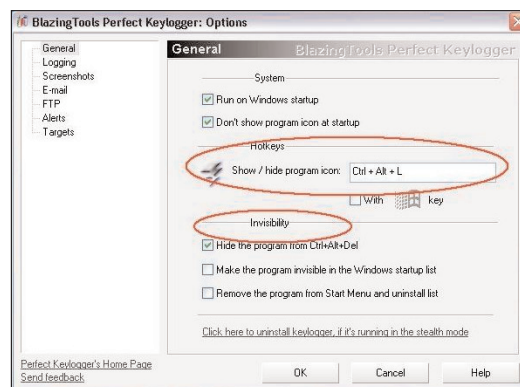
## Theft Account

### KeyLogger

Telah berapa kali diulas tentang program perekam hantakan keyboard yang satu ini di majalah kesayangan kita ini. Keylogger merupakan awalnya sebagai *Parental*

*Watch* atau sebuah alat yang bisa memantau kegiatan seseorang anak di internet, sehingga orang tua pun bisa memperhatikan situs mana saja dan apa saja yang dilakukan anaknya ketika berselancar. Check and re-check apakah anaknya benar-benar surfing ke web-web pelajaran atau malah menjelajah ke situs-situs yang mengarah urusan pornografi.

Keylogger pada awalnya digunakan oleh perusahaan-perusahaan untuk memantau pekerjaan karyawannya. Seorang manajer bisa menaruh keylogger disetiap PC client karyawan, dengan begitu ia dapat menganalisa apa saja yang dilakukan karyawannya sehari-hari.



Gambar 1. Blazing Perfect Keylogger

Namun sebuah penyimpangan terjadi ketika penggunaan keylogger menjadi sebuah alat mata-mata (SpyTools) dimana tidak lagi untuk memantau pekerjaan ataupun lainnya, kini keylogger digunakan untuk memantau password ataupun rekening lainnya.

Dalam contoh kasus di atas ketika seseorang menjadi korban kebocoran data karena sembrono mengakses Internet Banking tanpa disadari bahwasannya komputer yang digunakan mengandung program keylogger. Apapun yang diketikkan di atas keyboard pun terekam.

Keylogger pun mengalami kemajuan hingga semakin canggih, mulai dari kemampuan mematikan antivirus dan spyware, rekam layar (screen capture), OnClick screen capture (merekam gambar ketika mouse di klik pada point), send email, invisible by taskmanager, dan lainnya.

Diperlukan *security patching* dilakukan dari sisi nasabah dan bank. Dari sisi nasabah dengan menggunakan **anti-spyware**, **antivirus**, **IDS**, dan lainnya. Sedangkan dari sisi bank menggunakan **Virtual Keyboard**, **Slide Down Menu Input**, **Randomize PIN request**, dan lain-lain.

Semua itu tetap saja bisa dipatahkan, contoh dari sisi client yaitu antivirus dan antispyspyware pun sudah tidak

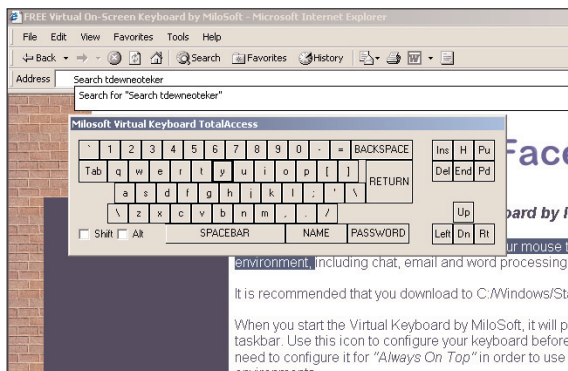


mampu lagi menangani keylogger terbaru. IDS hanya menyaring serangan luar dan tidak men-scan file yang masuk. Apalagi kalau yang digunakan itu bukan software keylogger, melainkan **Hardware Keylogger** yang ditanamkan diantara **port jack** dari Keyboard ke Port Motherboard, dengan begini oprek-oprek **registry** ataupun sistem pun tidak bisa menangkalnya.



Gambar 2.  
Hardware KeyLogger

Penggunaan **Virtual Keyboard** ataupun **Slide Down Menu Input** tidak dapat menangani pencurian akses, hanya dengan **Shoulder Surfing** maka teknik itupun bisa dipatahkan. Apalagi ketika mengakses di Warnet dimana lokasi PC yang berseberangan dan bersebelahan memudahkan anda melakukan Shoulder Surfing, dan parahnya lagi apabila di sisi komputer client ini sedang melakukan input data melalui virtual keyboard dan di seberangnya adalah user yang sedang menggunakan webcam maka secara otomatis Virtual Keyboard itu pun akan terlihat, dan rekeningpun bocor.



Gambar 3. Virtual keyboard

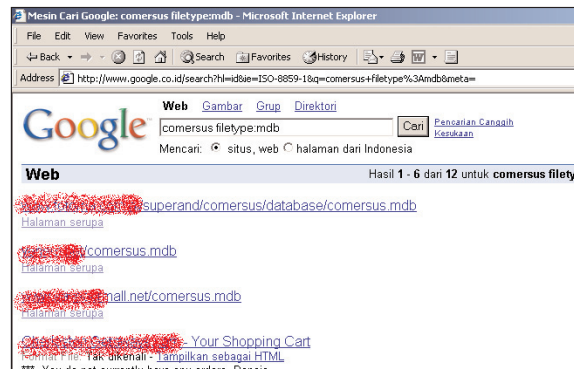
Randomize PIN request yang mengharuskan anda mengingat lebih banyak lagi kata-kata di kepala selain password, disini anda harus memasukkan angka-angka yang ada dalam pin anda dengan acak oleh sistem ini. Misalnya anda memiliki pin 666777 dan diminta memasukkan digit pertama, ketiga, dan keenam maka anda masukan 667.

Permasalahan keylogger merupakan masalah pertama yang harus dipecahkan oleh kedua belah pihak baik nasabah maupun bank. Dengan penggunaan alat seperti KeyBCA dapat menjadi salah satu pemecahan masalah ini, karena menggunakan PIN secara acak pada setiap kali transaksi dilakukan dan nasabah wajib memasukkan PIN tersebut, jadi ketika data rekeningnya dicuri maka rekeningnya tidak dapat dipakai untuk transaksi apapun, paling tidak hanya melihat jumlah saldo.

### Password Matching & Guessing

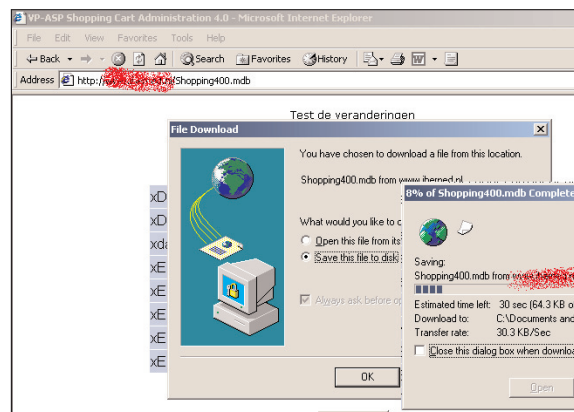
Password matching atau dengan kata lain mencocokkan password adalah cara lain yang digunakan untuk mencuri rekening Internet Banking. Memang kelihatannya memakan waktu dan terkesan tidak mudah, namun jangan salah dengan cara ini beberapa kasus pencurian rekening Internet Banking menggunakan cara ini.

Yang dilakukan pertama kali dalam pencurian rekening ini adalah dengan mencari database-database dari sebuah **e-shop** dimana yang paling banyak saat ini yang terjadi kebocoran data dengan pencurian database adalah software **e-commerce VP-ASP** dengan bug-nya yang tiap berganti versi juga berkembang. Biasanya trik yang dilakukan pertama kali untuk mencari target yang **vulnerable** akan bug ini adalah dengan mencari di google atau dengan kata lain menggunakan trik **Google hack**.



Gambar 4. Memanfaatkan Google mencari database e-shop

Dengan memasukkan sejumlah keyword di Google search engine **inurl: shopdisplayproducts.asp site:com** maka ketika dilakukan pencarian oleh Google, web-web yang muncul adalah web yang berakhiran dengan **.com** dan memiliki atau mengandung **shopdisplayproducts.asp**. Dari sini akan dilakukan penetrasi terhadap sistem, dimana dengan menggantikan kata-kata **shopdisplayproducts.asp** dengan **shopdbtest.asp** akan terlihat lokasi database, dan langsung bisa di download. Yang paling rawan akan teknik ini adalah dengan menggunakan **bug comersus** yang langsung terlihat direktori dan file databasenya.



Gambar 5. Mengambil file database

Lalu ketika database sudah di download maka selanjutnya adalah dengan mencari table customer dan mencari field Email dan password. Kebiasaan para pengguna internet dan bahkan hampir semua orang adalah menggunakan password yang sama untuk beberapa rekening penting, maka ketika si intruder ini telah melisting email dan password tersebut, selanjutnya ia tinggal mencocokkan email login dan password ke servis email customer.

Dan ketika dapat sebuah email yang di dalamnya berisi data-data perbankan, rekening belanja, sampai nomor

## NeoTekno

kartu kredit. Maka yang selanjutnya dilakukan adalah mencocokkan login rekening yang terdapat dalam email itu ke Internet Banking. Jika gagal, email-email korban lainnya sampai menemukan hasil yang diinginkan.

Memang trik ini sangat lama, dan kurang akurat, namun masih saja ada yang menjadi korban trik ini.

### Scamming/Phising

Scamming/phising pada dasarnya merupakan sebuah metode penipuan dimana seseorang dengan kemampuan web design yang bagus bisa membuat sebuah web tiruan terhadap web asli Internet Banking, kemudian membuat nama domain yang hampir sama dengan yang asli.

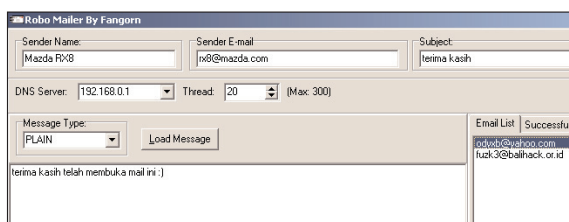
Seperti kejadian yang pernah menimpa KlikBCA.com dengan pelesetan menjadi KilkBCA.com maka nasabah yang sembrono dan tidak menyadari akan menjadi korban.

Orang biasa juga bisa membuat web tiruan ini hanya dengan bermodalkan sebuah program **website copier** atau dengan **HTTrack**, mendownload seluruh link dan disain secara utuh dari web asli tersebut dan menyimpannya di komputer pribadi, lalu dengan merubah sedikit kode yang ada di halaman web yang telah di download tadi, maka jadilah sebuah **scam site**.

Lain lagi dengan scam yang memang didesign sedemikian rupa tanpa mengikuti web aslinya, dengan tujuan orang agar menyetorkan uangnya ke web ini. Misal scam site dengan menawarkan produk-produk yang lebih murah dibandingkan harga pasaran, maka secara logika orang-orang akan mengunjungi dan membeli produk itu tanpa pikir panjang.

Namun upaya scamming ini takkan terlalu berhasil apabila para **scammer** ini belum melakukan iklan-iklan di internet, dan juga melakukan phising kepada email-email orang lain yang berpotensi memiliki atau akan mendaftar di web scam.

Scammer ini mengiklankan dengan berbagai macam trik, umumnya mereka menggunakan sebuah mail bot atau lebih dikenal dengan "mailer" sebuah coding web yang dapat mengirim ke banyak alamat e-mail dan isi bodynya bisa menerima dan menterjemahkan coding HTML ke dalam disain web. Jadinya ketika email phising ini diterima calon korban, maka yang terlihat bukanlah rangkaian *coding*, melainkan sebuah halaman website yang sudah jadi, dan melakukan rekayasa atau dengan teknik social engineering mengajak calon korban untuk mengunjungi dan melakukan login maupun mendaftar.



Gambar 6. Memanfaatkan program mailer bot

Terkadang ada juga scammer yang nakal, dengan memasukkan sebuah script khusus dibelakang webpage scam tadi agar komputer korban menerima sebuah program yang bisa merekam aktifitas (spyware) dan mengirimkan lognya ke email si scammer ini. Dengan begitu apabila nantinya korban akan melakukan login ke web asli, maka scammer ini bisa tahu login yang sudah diganti

passwordnya ataupun hal lainnya yang bersifat ekonomi.

### Shoulder Surfing

Telah dibahas sebelumnya bahwa dengan shoulder surfing ini, sistem antispyware seperti virtual keyboard dan rekannya dapat terpatahkan. Namun apa itu shoulder surfing? Apa hubungannya dalam pencurian rekening?

Shoulder surfing merupakan teknik pencurian rekening dimana seseorang mencuri password/akses dengan melihat langsung kepada layar komputer target, nantinya ketika si korban melakukan login dengan virtual keyboard maka dengan terang dan jelas, pengintai dapat mengintip username dan password dan langsung mencatatnya ke secarik kertas atau ponsel.

Apalagi ketika anda di warnet, kantor, ataupun kampus yang dimana orang-orang ramai berseliweran, dan diantara mereka itu anda tidak dapat menebak orang yang melakukan shoulder surfing. Shoulder surfing cukup sulit dilakukan karena dengan akses fisik ini dapat tertangkap basah. Untuk itu keahlian mengintip memang sangat diperlukan dalam teknik shoulder surfing ini.

### Theft Account by Peer-2-Peer

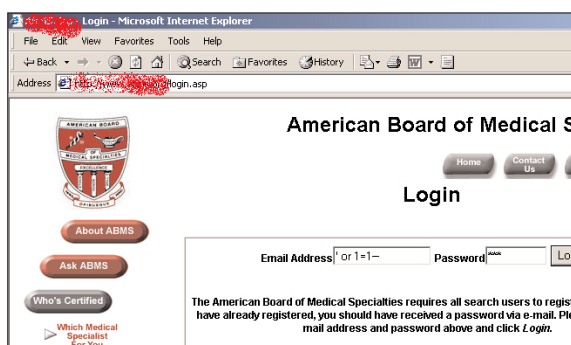
Peer to peer (P2P) merupakan teknologi untuk bertukar file (file sharing) dimana anda dapat mencari file-file yang anda inginkan, seperti MP3, film, data, dan lainnya. Namun teknologi ini dapat menjadikan sebuah ancaman ketika seseorang menyimpan data-data penting khususnya informasi login Internet Banking, maka dapat dengan mudah file ini dicuri orang melalui program P2P ini.

Hanya dengan mencari sebuah kata di dalam **search box P2P** maka apapun yang anda cari akan muncul, terlebih lagi ketika anda mencari file dengan nama paypal, **password**, **account**, **acct**, **pwd**, **passwd**, dan lain sebagainya. Yang akan anda temukan adalah sejumlah rekening Internet Banking yang mungkin saja masih aktif statusnya.

### SQL Injection

Teknik hacking yang lawas ini masih dalam urutan pertama dalam ancaman Internet Banking, bagaimana tidak yang diancam langsung ke dalam databasenya. Teknik SQL Injection telah dibahas di NeoTek sebelumnya.

SQL Injection berpengaruh pada **input box login**, jadi ketika melakukan akses Internet Banking maka yang dijumpai pertama kali adalah halaman akses dengan form input login. Nah, disini SQL Injection dapat meracuni **Query SQL** yang sudah ada dengan meng-**escape query** yang sudah ada tersebut dan membuat query baru yang dapat memungkinkan kita masuk ke dalam halaman member dari Internet Banking tersebut.



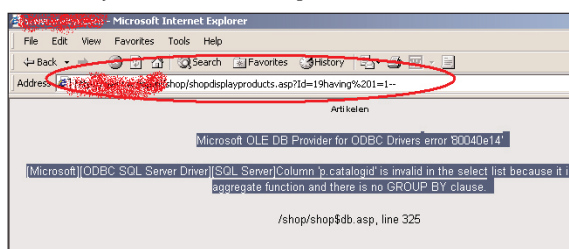
Gambar 7. SQL Injection pada input box

Dengan login ' or '=' , ' or 1=1-- atau ' or '1'='1' maka SQL query tersebut teracuni dan mempersilahkan untuk memasuki halaman user ataupun admin tanpa ijin yang sah. Ini dikarenakan kurangnya perhatian programmer pada **secure coding SQL**. Biasanya sebuah query login seperti ini,

```
SQL = "SELECT C=COUNT(*) FROM users where pass=''" & pass & ""
and user=''" & user & ""
```

Lalu dengan memasukan string tadi maka query di atas akan berubah menjadi **SELECT \* FROM users where pass='test' and user='test' OR '1' = '1'** yang artinya *data-base memilih semua value di dalam table user dimana field pass adalah 'test' dan user adalah 'test' atau 1=1 atau dengan kata lain dari SQL 1=1 adalah true*, sehingga query tadi mengijinkan masuk karena value-nya benar, lalu abaikan query selanjutnya karena tanda -- (double strip) dalam SQL berarti mengacuhkan apapun di belakangnya. SQL Injection tidak hanya terjadi pada input box, melainkan pada **URL value variable**. Dimana melakukan SQL injection ini setelah adanya value dari webserver, contoh **www.ibanking.com/article/ news.asp?id=1** nah **id=1** tersebut adalah value dari variable yang telah di tetapkan di *coding* web tadi. Lalu dengan memasukkan SQL query kotor tadi ke belakang value itu maka akan terlihat pesan **error SQL server** web tersebut.

**www.ibanking.com/article/news.asp?id=1 or 1=1--** ini akan menjadi awal mula malapetaka.



Gambar 8. SQL Injection pada input URL address

SQL injection juga tidak hanya inject query melulu, di dalam MS SQL terdapat **Stored procedure** dimana intruder dapat menjalankan **cmdshell** dari web tersebut untuk mencari data-data para nasabah. Beberapa stored procedure yang berbahaya antara lain:

- xp\_cmdshell - execute shell commands
- xp\_enumgroups - enumerate NT user groups
- xp\_logininfo - current login info
- xp\_grantlogin - grant login rights
- xp\_regdeletekey - registry manipulation

Dengan injeksi seperti ini kepada stored procedure **exec master..xp\_cmdshell 'ping 10.10.10.10'** maka server web tersebut akan mengirimkan paket, dan bisa membuka port tertentu dengan menaruh dan menjalankan **netcat**.

### Cyber Fraud

Cyber fraud atau istilah lainnya carding, juga termasuk ancaman dalam dunia E-Banking. Karena apabila seorang carder mempunyai akses rekening Internet Banking dengan menggunakan cara-cara di atas, maka dengan leluasa dan mudah menggunakan akses tersebut untuk membeli apapun di jagat internet atau melakukan transfer uang ke rekening pribadinya.

Lucunya, oleh para carder akses Internet Banking curian yang dimilikinya dapat ditukar dengan akses lain kepada sesama carder atau menjualnya.

Selain carding, **scamming** juga salah satu jenis cyber fraud. Dikarenakan sifatnya yang memang menipu para nasabah bank untuk mendaftar ataupun login ke dalam situs scam itu. Selain bisa juga membuat situs-situs donasi, kasus ini baru saja terkuak ketika setelah terjadinya bencana alam Tsunami. Beberapa web yang menyatakan akan menyalurkan dana dari orang-orang yang ingin menyumbang melalui internet banking, ataupun credit card.

Maret tahun 2005, terjadi sebuah kasus **scam** terbesar di Indonesia dimana para pelaku yang berjumlah 5 orang ini yang berdomisili di **Medan** membuat sebuah **scam site** dengan menawarkan produk Mobil Ferrari dengan harga yang jauh lebih murah dibanding pasaran dunia yaitu sekitar US\$55,000. Hal ini ditanggapi oleh seseorang yang berasal dari **Kuwait** dan berdomisili di **Bandung**. Transfer sejumlah uang dilakukan ke para pelaku scamming ini, ketika uang sudah diterima scammer ini, Ferrari yang ditunggu tak kunjung datang, akhirnya Polisi pun bertindak dan melacak pelaku dengan mengecek nomor rekening yang diberikan kepada korban. Pelacakan yang bekerja sama dengan pihak bank, berhasil menangkap para pelaku. Barang bukti US\$55,000 pun sudah berubah fisik menjadi sebuah mobil Suzuki Aerio, peralatan elektronik, laptop, dan lain-lain.

Nigerian Mail, salah satu jenis scamming dan juga merupakan salah satu bentuk cyber fraud. Banyak yang menjadi korban nigerian mail, modusnya dengan meminta dana kepada para nasabah Internet Banking, dengan bujukan harta karun yang terpendam. Dan ketika yang dijadikan calon korban merespon positif email tersebut, maka permintaan akan sejumlah uang yang alasan penggunaannya untuk dana eksplorasi mereka untuk mengambil harta tersebut. Dengan di iming-imingi pembagian hasil yang menggiurkan biasanya korban langsung mengikuti keinginan pelaku penipuan tersebut.

### Money Laundering

Kejahatan Money Laundering merupakan lagu lama di dunia perbankan, dikarenakan proses pencucian uang ini sangat sering terjadi dan hampir tak terlihat publik. Dan bukti pun bisa dengan mudah dihilangkan.

Contoh kasus kejahatan Money Laundering ini adalah melakukan transfer sejumlah uang dari rekening Internet Banking curian ke rekening palsu intruder, lalu ketika keadaan sudah memungkinkan maka uang yang berada dalam rekening palsu ini kemudian ditarik ataupun ditransfer langsung ke rekening aslinya.

Money Laundering sendiri sudah mendapatkan perhatian serius dimata hukum Indonesia, terbukti dengan dikeluarkannya undang-undang tentang pencucian uang. Dan bank-bank di Indonesia pun sudah bekerja sama dengan pihak kepolisian dalam memerangi pencucian uang ini.

### Cegah Tangkal

Seperti yang telah dipaparkan sebelumnya merupakan berbagai macam aktifitas sisi gelap dari E-Banking dan tidak hanya itu. Selanjutnya yang dibutuhkan adalah langkah-langkah pencegahan.

Pencegahan dini dan penerapan *security awareness* pada diri sendiri merupakan hal yang paling penting dalam menjaga rahasia E-Banking anda. Ada daftar 10 besar



## NeoTekno

kerawanan aplikasi web, dalam list ini mudah-mudahan anda yang memang seorang administrator system perusahaan dapat menganalisa sistem tersebut dan melakukan **penetration testing** untuk mencegah hal-hal yang tidak diinginkan semua orang.

Berikut daftarnya yang dibuat oleh **The Open Web Application Security Project** (OWASP) [www.owasp.org](http://www.owasp.org)

- **Unvalidated Parameters**  
Informasi dari web request belum di validasi sebelum digunakan oleh aplikasi web. Bahayanya **input validation** telah digunakan untuk menyerang server backend dari aplikasi web tersebut. **SQL Injection** atau **CGI Scripting** merupakan contoh dari kelemahan aplikasi web ini
- **Broken Access Control**  
Buruknya design dari web dapat menyebabkan intruder yang tidak sah dapat masuk ke halaman nasabah yang ter-autorisasi, sehingga intruder dapat melihat rekening nasabah tersebut atau melakukan hal-hal lainnya.
- **Broken Rekening and Session Management**  
Rekening yang telah tersahkan dan **login session** tidak terproteksi dengan tepat, sehingga intruder dapat menggunakan informasi tersebut untuk masuk ke dalam internet banking secara tidak sah. Contohnya adalah **Cookies Theft**.
- **Cross-Site Scripting Flaws**  
Cara ini lebih dikenal dengan nama **XSS** dimana melakukan input dan menanam script pada aplikasi web untuk mencuri rekening login dan lalu mengirimkan ke server si intruder, dan melakukan hal lainnya dengan XSS ini.
- **Buffer Overflows**  
Penyerangan dengan **buffer overflow** dapat menyebabkan sistem menjadi crash lalu ketika crash ini berlangsung, pengambil alihan sistem dapat terjadi dengan menjadi user dengan privilege setara admin.
- **Command Injection Flaws**  
Aplikasi web dapat memasukkan parameter-parameter kotor ke dalam sistemnya tanpa disaring, dan ini dapat menyebabkan OS-nya menjadi tereksplorasi contohnya adalah **Unicode Bug**.
- **Error Handling Problems**  
Kondisi pesan kesalahan yang muncul ketika dalam keadaan normal tidak tertangani dengan benar. Dengan informasi ini maka intruder dapat mengetahui informasi sistem tersebut dan melakukan tindakan lainnya.
- **Insecure Use of Cryptography**  
Aplikasi web biasanya menggunakan fungsi **kriptografi** untuk mengamankan data dan informasi berharga. Fungsi ini dan kode yang terintegrasi telah membuktikan bahwa susah untuk di coding secara benar, dan sering menghasilkan proteksi yang lemah.
- **Remote Administration Flaws**  
Banyak aplikasi web sekarang ini yang memungkinkan administrator web untuk mengakses ke dalam **WebSite Control Panel** dengan web interface. Dan jika menu administrasi ini tidak dilindungi dengan aman maka, seorang intruder dapat diartikan bisa menyerang dengan mudah dan menguasai sistem tersebut.
- **Web Application and Server Misconfiguration**  
Menggunakan prosedur dalam mengkonfigurasi server dengan aman sangat dibutuhkan dan merupakan hal yang sangat kritis karena server memiliki banyak

konfigurasi dimana setiap konfigurasinya berpengaruh kepada sistem dan keamanannya.

Berapa Security Awareness kepada para nasabah dan perlu diperhatikan dan juga diterapkan antara lain:

- Merubah secara berkala Password Internet Banking tersebut, agar kemungkinan pencurian rekening internet banking menjadi lebih kecil.
- Menggunakan password yang panjang, paling tidak minimal 8 karakter, dan menggunakan kombinasi huruf dan angka.
- Tidak menggunakan password yang sama pada setiap rekening penting, baik itu rekening e-mail, rekening perusahaan, dan lainnya.
- Tidak menggunakan password yang berkaitan dengan pribadi, misalnya nama belakang yang digabung dengan tanggal lahir, nama pacar, merek mobil pribadi, nomor polisi mobil anda, dan lainnya. Ini dilakukan agar terhindar dari teknik **Password Guessing**.
- Menggunakan PC pribadi ketika melakukan transaksi rekening. Ini untuk menanggulangi pencurian rekening.
- Apabila login dari PC umum, maka sebaiknya lihat dulu kondisi warnet, keadaan komputer, lihat sistemnya, lakukan **simple penetration test** kepada komputer tersebut, misalnya menghapus folder, menginstalasi, dan lainnya, lihat task manager komputer tersebut apakah ada hal-hal yang mencurigakan yang berjalan di belakangnya. Monitor terus **performance taskmanager** dengan memperhatikan diagram yang memperlihatkan persentase memori, coba menekan klik dan apabila ketika mengklik mouse terjadi lonjakan dan begitu seterusnya maka patut dicurigai di komputer itu telah terpasang spyware. Lihat keadan warnet apakah penuh atau tidak, apabila penuh sebaiknya anda tinggalkan warnet atau menunggu untuk sepi, karena ketika warnet penuh shoulder surfingpun bisa dimanfaatkan untuk mencuri rekening anda.
- Waspadalah terhadap scam mail yang dikirimkan ke e-mail anda, untuk mencegahnya aktifkan opsi Header mail anda, dengan ini alamat pengirim dapat terlihat, jadi ketika ada email yang tidak dikenal dapat dilihat IP address-nya dari negara mana, berikut informasi lainnya.
- Jangan lupa untuk **LogOut** ketika sudah selesai melakukan transaksi di Internet Banking tersebut. Hal ini dilakukan untuk menghindari orang lain menggunakan rekening anda dan melakukan hal yang tidak-tidak.
- Kalau sempat, hapus semua **offline files, cookies**, dan **remove username** dan **password** di internet option.
- Jangan menuliskan password dan username rekening anda di secarik kertas, kalender, handphone, ataupun organizer anda, karena dapat dilihat oleh orang lain yang kebetulan sedang memakai alat-alat tersebut.
- Instal antispyware dan antivirus terbaru dan selalu rajin mengupdatenya agar terhindar dari program-program pengganggu.

Security Awareness memang perlu dilakukan dalam berinternet, tidak saja ketika melakukan **Online Banking**, dengan *security awareness* ini maka anda akan terhindar dari hal-hal yang tidak diinginkan. Jadi dengan tidak ter-lalu menggantungkan kepada bank.



# ADOBE PHOTOSHOP Colour Focusing

**Mempercantik photo** koleksi dengan memberikan efek tertentu. **Rafeequl Rahman Awan** (rafeequl@neotek.co.id) memberikan tips Colour Focusing untuk mempercantik photo koleksi anda.

## Membuat efek colour focusing.

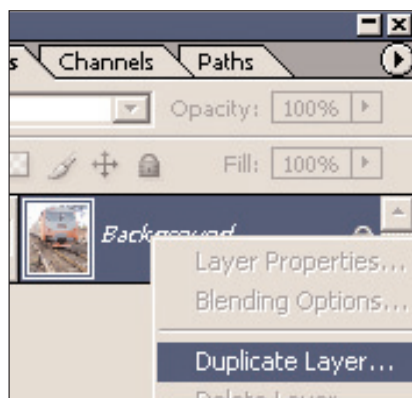
**B**ANYAK JALAN MENUJU ROMA, banyak juga jalan untuk melakukan focusing kepada suatu object. Focusing, maksudnya kita ingin memberikan suatu pusat perhatian dengan cara memberikan efek/teknik tertentu kepada suatu titik perhatian yang akan di jadikan fokus utama. Cara yang umum digunakan adalah dengan menjadikan suatu object menempatkan ukuran lebih besar atau dengan mengisolasinya dengan ruang tajam tertentu seperti yang biasa kita lihat pada foto model (model terlihat jelas sedangkan background-nya blur). Seiring dengan kemajuan jaman dan teknologi, cara cara lain kemudian dikembangkan. Salah satunya adalah dengan permainan warna. Dengan menghilangkan/mengurangkan satuasi warna background dan membiarkan atau malah mengekspos object utama. Cara ini yang akan coba kita praktekkan pada tutorial kali ini. Penulis akan memberikan fokus khusus kepada sebuah kereta yang sedang melintas, kemudian membiarkan sekeliling kereta menjadi hitam putih. Caranya cukup mudah untuk dipraktekan, baik bagi pemula sekalipun. Ada tool andalan yang akan kita gunakan disini. Yaitu masking, bagi anda yang belum mengerti apa itu layer masking penulis akan coba menjelaskannya terlebih dahulu. Seperti namanya, masking adalah topeng yang berfungsi untuk menyembunyikan semua/sebagian dari suatu layer. Layer masking boleh dikatakan bersifat grayscale, hanya mengenal warna dari hitam ke putih. Semakin gelap layer masking berarti layer yang bersangkutan akan semakin disembunyikan. Supaya memper-

jelas pemahaman anda mengenai ini semua mari kita mulai saja proyek kita kali ini.

- Pertama-tama buka photoshop dan buka file yang akan anda masking.

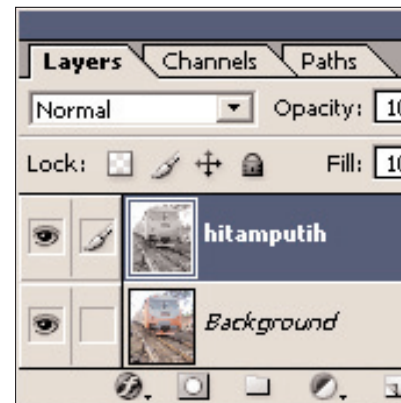


- Buat **duplikat layer** dari layer background, caranya klik kanan layer background kemudian pilih duplicate. Beri nama hitamputih.

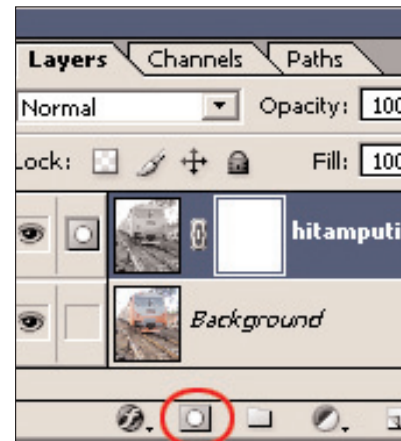


- Lalu **aktifkan layer** hitamputih.
- Pilih **image>Adjustment>Desaturate** atau bisa juga dengan kombinasi tombol Ctrl+Shift+U

Ketika anda melakukan ini maka layer yang bersangkutan akan menjadi hitam putih. Dan secara keseluruhan yang tampak di monitor anda adalah gambar yang sudah menjadi hitam putih. Tapi ingat layer background masih full color.



- Masih di layer hitamputih, sekarang tambahkan mask dengan memilih tombol **Add vektor mask**.



- Lakukan penyeleksian terhadap bagian gambar/foto yang akan anda jadikan sebagai fokus utama.

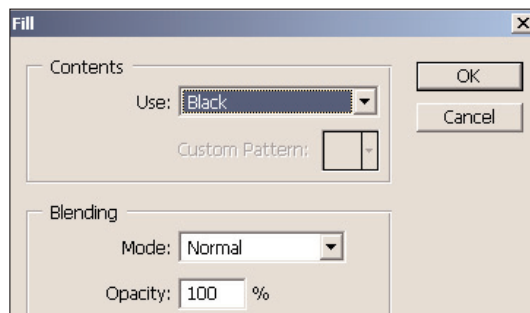
## NeoStyle

Pada kasus kali ini kebetulan penulis ingin menonjolkan kereta sebagai fokus utama.



*Tips: Anda bisa menggunakan lasso tool bila ingin melakukan seleksi terhadap objek yang sederhana, bila objeknya kompleks, gunakan bantuan pen tool untuk melakukannya. Penggunaan pen tool di luar bahasan artikel ini.*

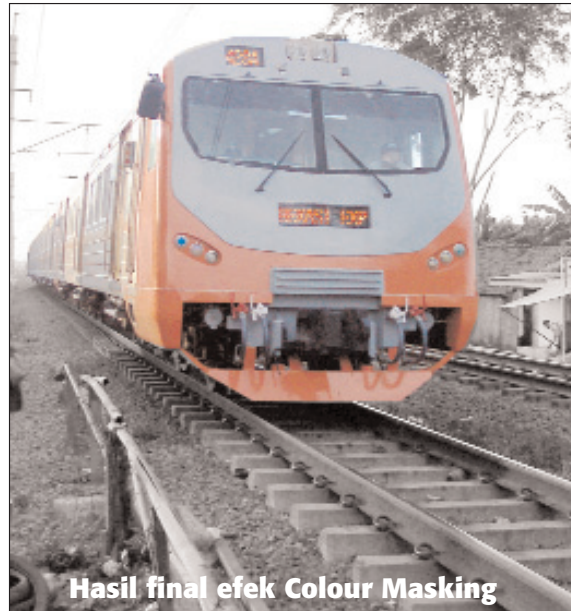
- Setelah kita selesai melakukan seleksi, pilihlah layer vector yang tadi sudah kita buat. Dengan keadaan seleksi yang masih aktif, isi/fill layer mask dengan warna hitam. Caranya klik menu **Edit> Fill>Black**.



- Nah sudah terlihat beda bukan. Object utama berwarna ceria tapi backgroundnya tetap hitam putih. Ini semua karena layer yang paling atas disembunyikan sebagian oleh layer mask, jadi seakan akan layer tersebut bolong.



- Sebagai pemanis, anda bisa tambahkan teknik **soft focusing** yang telah di bahas pada artikel NeoStyle pada edisi lalu.



## CD NeoTek Edisi Mendatang

### PANHAC Linux Security Auditor

**D**istro berbasis linux yang dipersiapkan untuk tujuan audit sekuriti (Security Auditor). Bagi anda yang berkecimpung dengan Teknologi Informasi yang ingin menjadi seorang security auditor, distro yang disuguhkan di edisi NeoTek mendatang (NeoTek Vol. VI - No. 03).

Pada beberapa waktu lalu, ketika acara kompetisi Hacking 2006 yang diberi nama PANHAC (Pazia National Hacking) 2006, distro ini disediakan bagi peserta yang mengikuti acara. Jadi bagi anda yang belum sempat mencoba distro tersebut, jangan lupa untuk memiliki NeoTek edisi mendatang.

Sesuai dengan namanya yaitu Security Auditor, fasilitas yang dimilikinya dikonsentrasikan pada peralatan untuk menguji sistem keamanan.

Distro ini juga cocok bagi anda yang ingin mengetahui mengenai hacking lebih mendalam, dengan tersedianya perangkat lunak (software) untuk urusan hacking, anda dapat menganalisa bagaimana sebuah sistem dibentuk, bagaimana sistem dapat ditembus, dan bagaimana memunculkan solusi bagi sebuah sistem yang dapat ditembus keamanannya.

*Tunggu apa lagi?*





## EASY MOSAIC Photo Mosaic

**Mempercantik photo** koleksi dengan memberikan efek tertentu. **Rafeequl Rahman Awan** (rafeequl@neotek.co.id) memberikan tips foto mosaic untuk mempercantik photo koleksi anda.

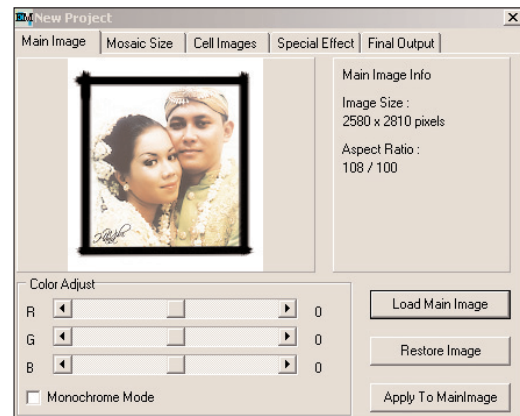
### Membuat efek mosaic dengan menggunakan Easy Mosaic.

**M**UNGKIN TERDENGAR ANEH pertama mendengar judul tutorial kali ini. Kita akan membuat photo dari photo. Maksudnya adalah membangun sebuah photo mosaic yang masing-masing mosaic-nya berasal dari foto juga. Baiklah, untuk mudahnya silakan lihat gambar dibawah ini. Disebelah kiri adalah gambar asli, dan di sebelah akan adalah gambar mosaic nya. Jika perhatikan lebih dalam, mosaic pembentuk gambar yang di sebelah kanan pada dasarnya adalah gambar-gambar juga, hanya saja disusun sedemikian rupa supaya bisa menyerupai dengan gambar asli. Dengan penempatan komponen-komponen mosaic yang tepat maka akan didapatkan kesan menyerupai gambar asli. Penempatan memperhatikan warna dan contrast dari tiap partikel mosaic. Yang tidak kalah penting adalah ukuran tiap partikel mosaic. Semakin kecil ukuran mosaic maka gambar akan semakin menyerupai aslinya, tapi sebaliknya, bila mosaic makin besar maka hasil akhir tidak begitu menyerupai. Walaupun bukan suatu keharusan tapi biasanya teknik ini dipakai untuk cetak besar, minimal untuk poster. Maksudnya adalah untuk memperkuat antara hasil mosaic secara keseluruhan dan detail tiap komponen mosaic.

Banyak alasan untuk melakukan manipulasi ini pada sebuah photo. Misalkan saja bila kita ingin membuat mosaic photo pengganti, nah komponen mosaic-nya bisa saja berupa kumpulan photo-photo pengganti mulai dari mereka pacaran hingga di pelaminan. Foto mosaic seperti itu bisa mengandung makna sebuah perjalanan cinta yang romantis. Menarik bukan?

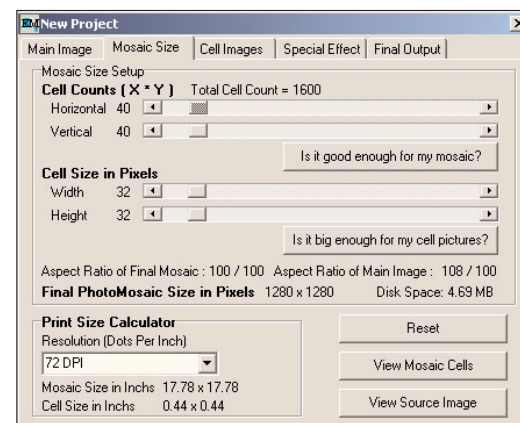
Bersyukurlah kita sekarang bisa membuatnya hanya dengan beberapa klik saja, karena dengan software Easy Mosaic kita tidak perlu lagi repot-repot melakukannya secara manual. Tinggal tentukan photo/image masternya, kemudian tentukan library/kumpulan photo/image yang nantinya menjadi komponen mosaic. Dan selanjutnya atur ukuran properti mosaic dan terakhir klik finish dan semuanya pun akan dilakukan oleh Easy Mosaic secara otomatis.

- Install Easy Mosaic, caranya cukup mudah hanya perlu next dan next saja.
- Kemudian jalankan Easy mosaic
- Pilih New, pada tampilan New Project, pilih load main images. Main Images adalah Foto/Images yang mau kita buat mosaic-nya.



Gambar 1. New project

- Setelah memilih MainImages, pindah ke tab selanjutnya yaitu Mosaic Size, setting ini sangat sangat fleksibel dan tergantung kebutuhan anda. Yang pertama Cell Counts adalah total banyaknya cell dari kiri ke kanan (horizontal) dan dari atas kebawah (vertikal). Yang kedua Cell size in pixell, opsi ini berfungsi untuk mengatur seberapa besar setiap cell. Yang terakhir adalah Resolusi, untuk hasil yang baik gunakan resolusi 300 DPI

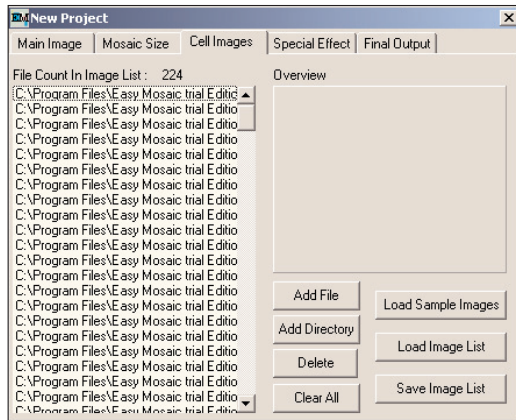


Gambar 2. Cell counts

- Lanjut ke tab Cell Images, di tab ini secara default EasyMosaic sudah memberikan sample images. Tapi

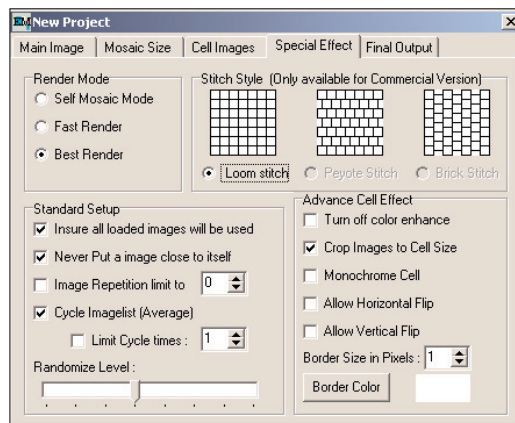
## NeoStyle

bila anda menginginkan gambar yang lain anda bisa menambahnya baik per file atau per folder sekaligus dengan mengklik tombol Add File/Add Directory



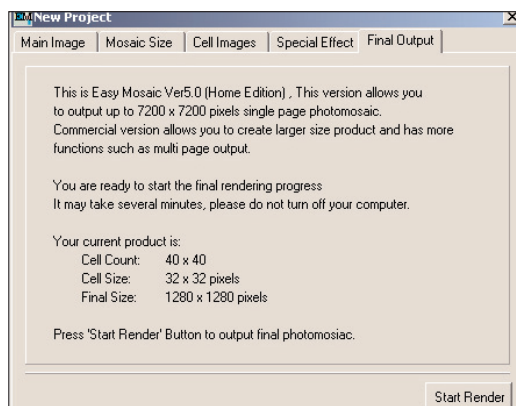
Gambar 3. Menambah file image/photo

- Pada tab special effects, anda dapat mengatur Mode Render yang terdiri dari 3 tipe dan best adalah yang terbaik. Kemudian tipe posisi penempatan cell, dan tingkat randomness pemunculan images dalam cell



Gambar 4. Special effects

- Terakhir bila semuanya dirasa sudah siap, maka anda



Gambar 5. Start render

tinggal mengklik tombol Start Render lalu biarkan EasyMosaic bekerja. Lama waktu render tergantung dari seberapa besar final image yang anda buat.

