

# PENGAMANAN PC dari Segala Ancaman

**Kenali berbagai ancaman PC Anda  
dan bagaimana mengatasinya**



**Edy Winarno ST, M.Eng**  
**Ali Zaki**  
**SmitDev Community**

[pustaka-indo.blogspot.com](http://pustaka-indo.blogspot.com)

# **Pengamanan PC dari Segala Ancaman**

pustaka-indo.blogspot.com

Sanksi Pelanggaran Pasal 72  
Undang-Undang Nomor 19 Tahun 2002  
Tentang HAK CIPTA

1. Barangsiapa dengan sengaja dan tanpa hak melakukan perbuatan sebagaimana dimaksud dalam Pasal 2 Ayat (1) atau Pasal 4<sup>9</sup> Ayat (1) dan Ayat (2) dipidana dengan pidana penjara masing-masing paling singkat 1 (satu) bulan dan/atau denda paling sedikit Rp1.000.000 (satu juta rupiah), atau pidana penjara paling lama 7 (tujuh) tahun dan/atau denda paling banyak Rp5.000.000.000 (lima miliar rupiah).
2. Barangsiapa dengan sengaja menyiarakan, memamerkan, mengedarkan, atau menjual kepada umum suatu ciptaan atau barang hasil pelanggaran hak cipta atau hak terkait sebagai dimaksud pada Ayat (1) dipidana dengan pidana penjara paling lama 5 (lima) tahun dan/atau denda paling banyak Rp500.000.000 (lima ratus juta rupiah).

# **Pengamanan PC dari Segala Ancaman**

**Edy Winarno ST, M.Eng  
Ali Zaki  
SmitDev Community**

**PENERBIT PT ELEX MEDIA KOMPUTINDO**



**KOMPAS GRAMEDIA**

## **Pengamanan PC dari Segala Ancaman**

**Edy Winarno ST, M.Eng**

**Ali Zaki**

**SmitDev Community**

©2014, PT Elex Media Komputindo, Jakarta

Hak cipta dilindungi undang-undang

Diterbitkan pertama kali oleh

Penerbit PT Elex Media Komputindo

Kelompok Gramedia, Anggota IKAPI, Jakarta 2014

nkfadli@elexmedia.co.id

121141463

ISBN: 978-602-02-4374-0

Dilarang keras menerjemahkan, memfotokopi, atau memperbanyak sebagian atau seluruh isi buku ini tanpa izin tertulis dari penerbit.

Dicetak oleh Percetakan PT Gramedia, Jakarta

Isi di luar tanggung jawab percetakan

# Kata Pengantar

Komputer ibarat rumah, jika rumah bisa kecurian, maka komputer bisa mendapatkan ancaman dari pihak luar. Karena itu, kewaspadaan merupakan hal wajib yang harus diperhatikan oleh semua pemilik komputer.

Banyak pemilik komputer yang tidak menyadari bahwa perlu adanya perhatian khusus ke masalah keamanan komputer. Buku ini menjelaskan beberapa bagian penting yang harus diperhatikan untuk menjaga keamanan komputer dari berbagai gangguan, serta meningkatkan keamanan dari sistem komputer rumah.

Setelah mempelajari buku ini, diharapkan Anda akan mampu menjauhkan komputer dari semua ancaman, sehingga komputer Anda aman terkendali.

Penulis menyadari bahwa buku ini tidak luput dari kesalahan dan masih jauh dari sempurna. Untuk itu, penulis membuka diri untuk segala bentuk tanggapan dan pertanyaan pembaca berkaitan dengan buku ini. Untuk berkonsultasi secara langsung dengan penulis, silakan layangkan email ke [winarno@smitdev.com](mailto:winarno@smitdev.com) atau [ali@smitdev.com](mailto:ali@smitdev.com).

Semarang, Mei 2014

Edy Winarno ST, M.Eng  
Ali Zaki  
SmitDev Community

# Daftar Isi

<b>Kata Pengantar.....</b>	<b>v</b>
<b>Daftar Isi.....</b>	<b>vi</b>

## **BAB 1 Pengamanan Firewall .....****1**

1.1 FirewallPAPI .....	2
1.2 iSafer .....	7
1.3 Windows Firewall .....	16

## **BAB 2 Pengamanan AntiVirus .....****21**

2.1 Anatomi AntiVirus .....	23
2.2 Mengenal Virus .....	25
2.3 Avira Antivir .....	26
2.4 ClamWin .....	35

## **BAB 3 Menghindari Ancaman Online.....****43**

3.1 File Transfer Protocol (FTP) .....	44
3.2 Hypertext Transport Protocol (HTTP).....	48
3.2.1 Metode Pemformatan HTML .....	48
3.2.2 Apa itu Script? .....	50
3.2.3 Scripting Berbasis Client.....	52
3.2.4 Scripting Berbasis Server.....	54
3.2.5 Serangan di Web dan Pencegahannya.....	55
3.3 Domain Name Service (DNS) .....	60
3.4 Dynamic Host Configuration Protocol (DHCP) .....	61
3.5 Konten Tak Layak.....	62
3.5.1 Family Safety.....	63
3.5.2 FoxFilter .....	66

## **BAB 4 Up to Date dengan Patch.....****69**

4.1 Apa Itu Patch?.....	70
4.1.1 Sumber Patch .....	71
4.1.2 Ukuran Patch .....	72
4.2 Hotfix .....	73

4.3 Service Pack.....	73
4.4 Windows Update.....	75

## **BAB 5 Email dan Ancamannya .....77**

5.1 Simple Mail Transfer Protocol (SMTP).....	77
5.2 Spam .....	78
5.2.1 Mencegah Spam .....	79
5.2.2 Cara Spammer Memperoleh Alamat Email .....	80
5.3 Tips Menghindari Spam .....	83
5.4 Menggunakan Email Gratisan .....	84
5.5 Menggunakan Spam Filter.....	86

## **BAB 6 Backup dan Restore .....93**

6.1 Backup MBR .....	93
6.1.1 HDHacker.....	94
6.1.2 MBR Wiz.....	97
6.2 Backup File.....	103
6.2.1 Instalasi Cobian Backup .....	103
6.2.2 Pengaturan Opsi Cobian Backup .....	106
6.2.3 Pembuatan Task Backup .....	119

## **BAB 7 Pengamanan Menggunakan Password .....127**

7.1 Peranan Password .....	127
7.2 Membuat Password Aman .....	128
7.3 Tips Membuat Password .....	131
7.4 Password Cracker .....	132
7.5 Pengecekan Kualitas Password .....	133
7.6 Password Generator.....	135

## **BAB 8 Download dan Instalasi Program .....139**

8.1 Free Download Manager.....	139
8.2 Download dengan Aman .....	145

## **BAB 9 Penggunaan Enkripsi .....149**

9.1 Mengenal TrueCrypt.....	149
9.2 Menginstal TrueCrypt.....	151
9.3 Membuat Kontainer Terenkripsi .....	153
9.4 Mounting File .....	159

<b>BAB 10 Membantai Spyware.....</b>	<b>167</b>
10.1 Mengenal Spyware .....	168
10.2 Advanced Spyware Remover .....	170
<b>BAB 11 Clean Uninstall.....</b>	<b>185</b>
11.1 Uninstall dengan Revo Uninstaller.....	185
<b>Tentang Penulis.....</b>	<b>191</b>

## BAB

# 1

# Pengamanan Firewall

Firewall atau “tembok api” merupakan istilah dalam dunia security yang bentuk fisiknya bisa berupa hardware atau software. Tujuan firewall untuk membuat aturan yang berguna memberi izin (permit /allow), menolak (deny), mengenkripsi (encrypt), dan mem-proxy lalu-lintas data di komputer antar domain yang berbeda.

Dengan demikian, firewall bertujuan mencegah hacker memasuki sistem komputer tanpa haki. Firewall menegakkan aturan kebijakan keamanan seperti halnya fungsi kartu akses dan pintu gerbang dalam sebuah gedung yang berguna untuk mengizinkan orang yang berhak untuk memasuki gedung dan menolak orang yang tak berhak memasuki gedung.

Untuk melengkapi fungsinya, firewall memiliki filter yang tidak akan mengizinkan materi-materi yang tidak terotorisasi atau berpotensi mengganggu sistem untuk memasuki sistem. Selain itu, firewall juga mencatat log pada upaya-upaya untuk memasuki sistem. Jika komputer Anda terhubung ke jaringan luar, baik jaringan lokal kantor, WAN, atau Internet, maka mau tak mau, wajib hukumnya menginstal firewall.

Sebuah firewall dapat memproteksi komputer dengan cara memeriksa tiap paket informasi yang lalu-lalang di jaringan. Bagaimana firewall mencurigai adanya paket-paket nakal? Caranya adalah dengan membaca alamat tujuan dari paket tersebut. Firewall mengandung *rule* yang menentukan alamat tujuan yang dibolehkan dan alamat tujuan yang tak diperbolehkan.

Jika sebuah paket ditujukan untuk alamat yang dilarang atau datang dari alamat yang dilarang, maka firewall akan menghentikan paket tersebut. Begitu pula jika paket menuju alamat yang valid, namun port-nya tidak diketahui atau dilarang, maka firewall juga akan menyetop paket tersebut. Firewall bisa juga mencatat/tracking paket-paket yang keluar dari komputer.

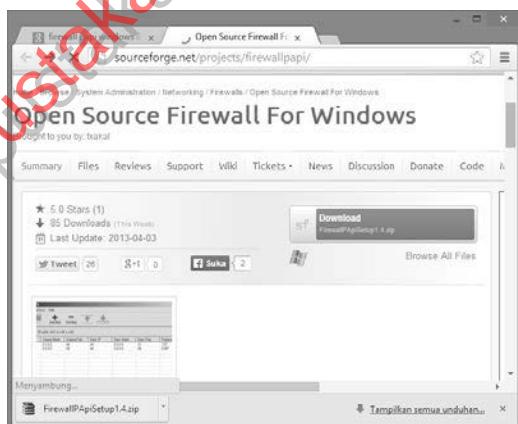
Dengan adanya penyeleksian paket-paket data yang lalu-lalang, maka firewall dapat digunakan untuk mencegah ancaman-ancaman aktif yang ada di komputer, seperti worm dan virus. Software-software jahat ini sering kali memasuki komputer menggunakan cara yang licik, seperti melalui port tertentu yang umumnya tidak termonitor.

## 1.1 FirewallPAPI

FirewallPAPI merupakan sebuah firewall yang bersifat opensource dan bisa dijalankan di versi Windows 2000 ke atas, termasuk Windows 7 dan Windows 8.

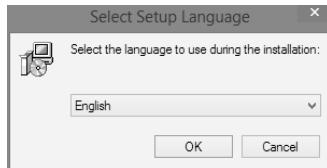
Lisensi yang digunakan untuk software ini adalah *GNU General Public License* (GPL). Software ini cukup sering di-update, sehingga masih relevan untuk sistem operasi modern sekarang.

1. Download FirewallPAPI dari <http://sourceforge.net/projects/firewallpapi/>. Ekstrak file hasil download dan jalankan instalasi.



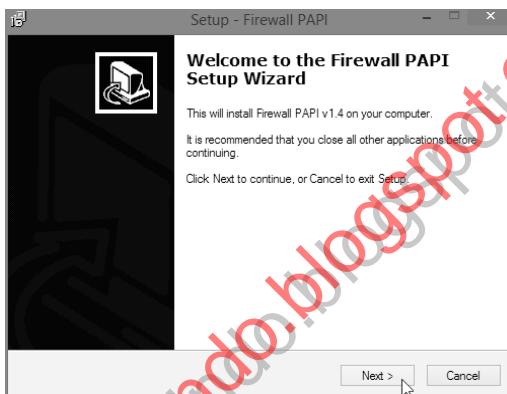
Gambar 1.1 Software Firewall PAPI

2. Pilih English di **Select the language to use during the installation**, klik OK.



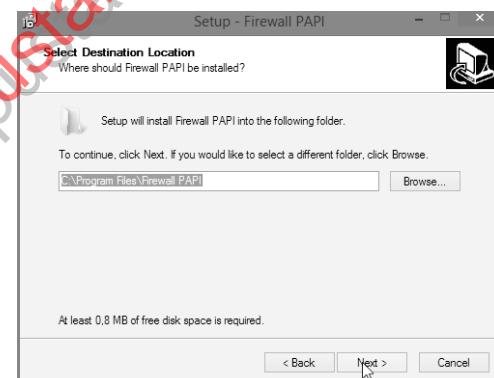
*Gambar 1.2 Pilih bahasa instalasi*

3. Muncul jendela **Welcome to the Firewall PAPI Setup Wizard**, klik Next.



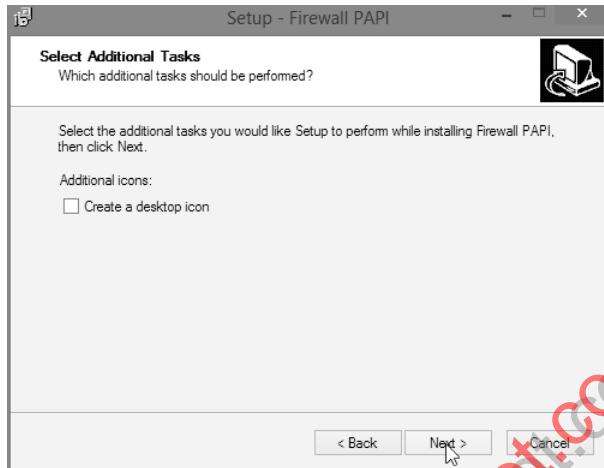
*Gambar 1.3 Jendela Welcome to the Firewall PAPI Setup Wizard*

4. Pilih lokasi instalasi di **Select Destination Location**.



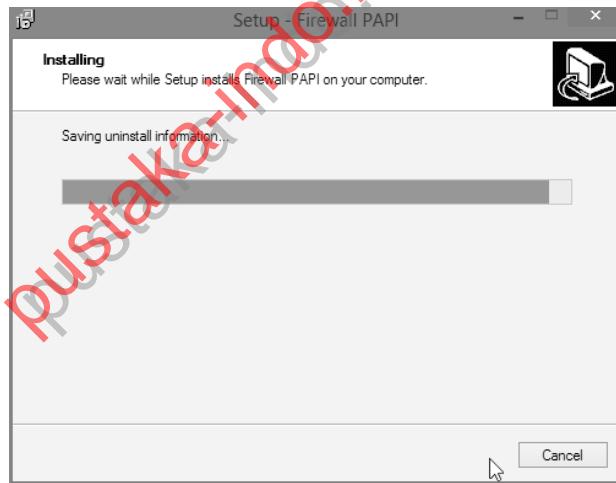
*Gambar 1.4 Pemilihan lokasi instalasi di Select Destination Location*

5. Di **Select Additional Tasks**, klik **Next** langsung.



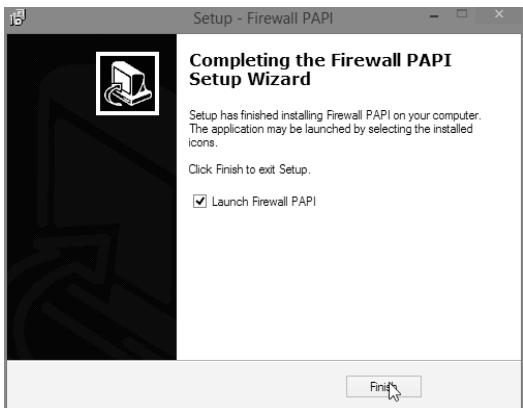
*Gambar 1.5 Tahapan Select Additional Tasks*

6. Rekap instalasi ditampilkan di **Ready to Install**. Klik pada tombol **Install**.
7. Tunggu hingga instalasi selesai berlangsung.



*Gambar 1.6 Instalasi tengah berlangsung*

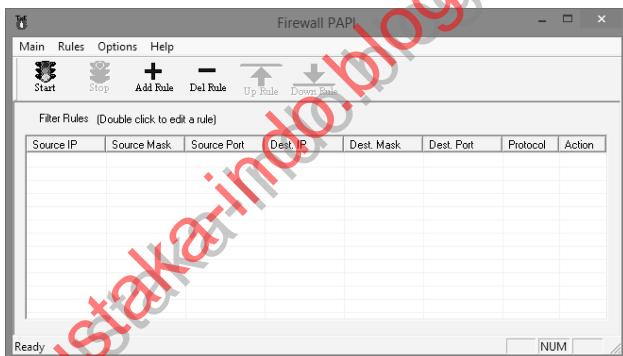
8. Di akhir instalasi, cek pada **Launch firewall PAPI** dan klik **Finish** untuk mengakhiri dan menjalankan Firewall PAPI.



Gambar 1.7 Akhir instalasi Firewall PAPI

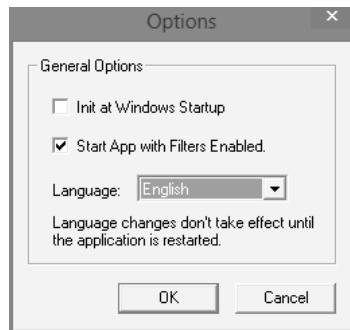
Setelah diinstal, bisa digunakan dengan cara seperti berikut:

1. Eksekusi Firewall PAPI.
2. Muncul jendela Firewall PAPI seperti berikut.



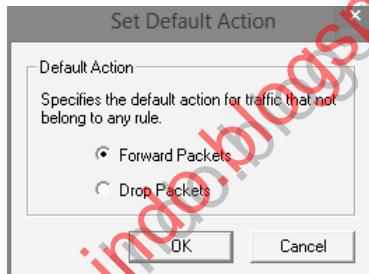
Gambar 1.8 GUI dari jendela utama Firewall PAPI

3. Untuk menjalankan firewall guna memonitor lalu-lintas data, klik pada button **Start** di toolbar yang tandanya seperti lampu lalu-lintas.
4. Penyetelan opsi untuk firewall dapat dilakukan dengan mengklik menu **Options** > **Set Options**. Lalu, Anda bisa mengeset apakah firewall dimulai sejak Windows Startup (**Init at windows startup**) dan juga memulai aplikasi dengan filter otomatis terpilih (**Start app with filters enabled**).



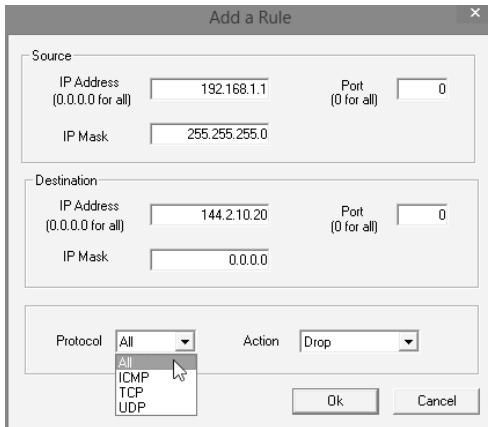
*Gambar 1.9 Pengaturan di General Options*

5. Inti dari aplikasi firewall adalah penentuan action untuk rule, yaitu aturan untuk menentukan bagaimana perlakuan standar terhadap data. Caranya, klik menu **Rules > Set Default Action**.



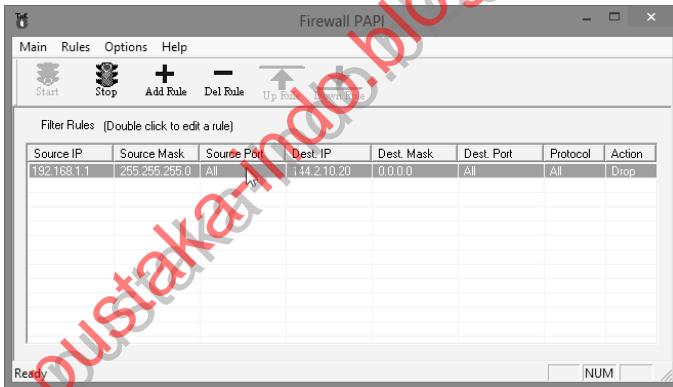
*Gambar 1.10 Pengaturan setting action default*

6. Kemudian, buat rule dengan mengklik button **Add a Rule**. Anda bisa menentukan IP address sumber atau IP address tujuan yang akan difilter.
7. Selain itu, tentukan protokol yang hendak difilter beserta port-nya. Lalu, tentukan action untuk traffic yang memenuhi persyaratan-persyaratan yang ada. Misalnya, Anda ingin memblok akses terhadap website tertentu, maka tentukan IP address dari server di **Destination** dan set action ke **Drop**. Klik button **OK** untuk memasukkan rule tersebut.



Gambar 1.11 Penentuan Add a Rule

- Rule yang sudah terbuat terlihat di bagian Filter Rules. Anda bisa mendefinisikan rule sebanyak yang Anda butuhkan. Untuk menghentikan layanan firewall, klik pada button Stop.



Gambar 1.12 Rule sudah dipakai, dan firewall diaktifkan

## 1.2 iSafer

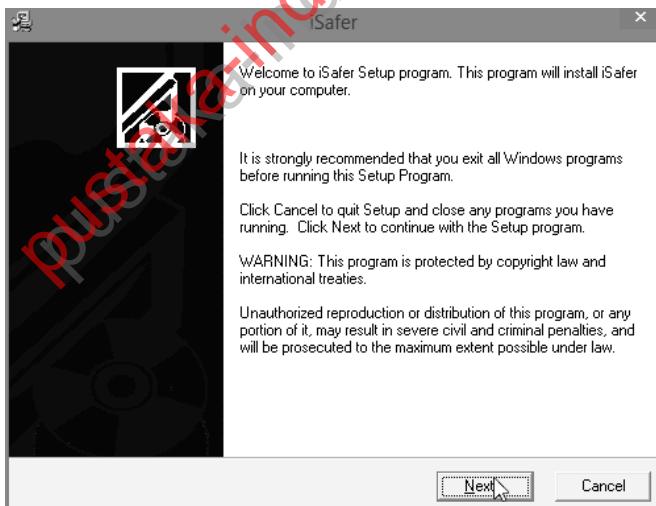
Download iSafer dari <http://sourceforge.net/projects/isafer/>, atau Anda bisa langsung melihat file-file yang dirilis dari iSafer di [http://sourceforge.net/project/showfiles.php?group\\_id=118375](http://sourceforge.net/project/showfiles.php?group_id=118375).



**Gambar 1.13 Halaman download iSafer**

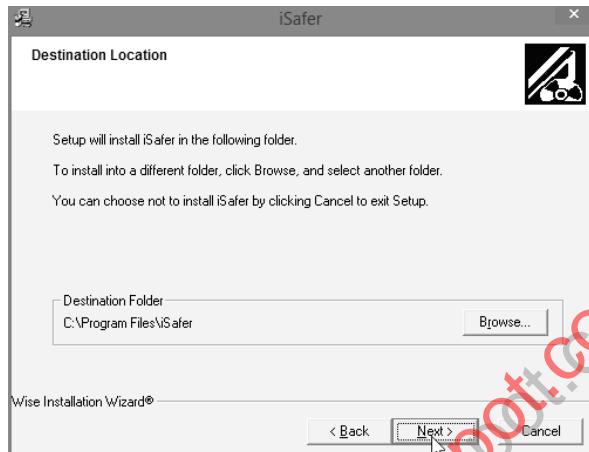
Selanjutnya, install iSafer dengan menggunakan langkah-langkah berikut ini:

1. Klik dua kali pada file executable installer yang diunduh. Di **Welcome to iSafer Setup Program**, klik **Next**.



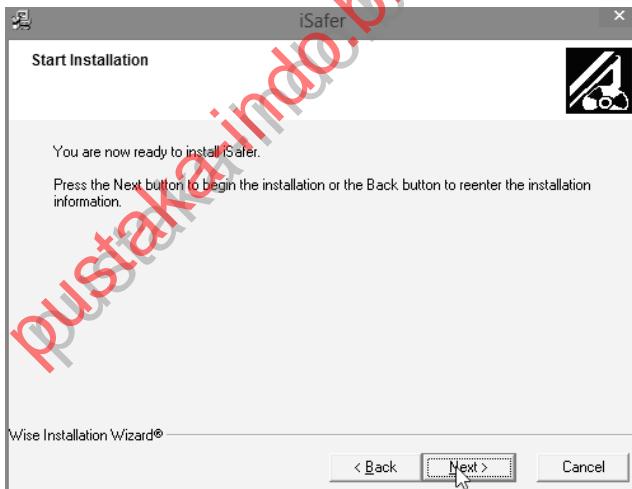
**Gambar 1.14 Jendela Welcome to iSafer setup program**

2. Berikutnya adalah **Destination Location** untuk menentukan lokasi instalasi. Klik **Next** untuk memulai inti tahapan instalasi dari program iSafer tersebut.



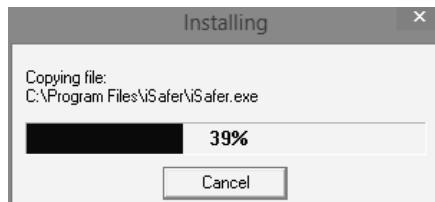
*Gambar 1.15 Penentuan Destination Location program iSafer*

3. Di **Start Installation**, klik **Next**.



*Gambar 1.16 Klik Next di Start Installation*

4. Tunggu hingga file instalasi disalin dan diinstal.



Gambar 1.17 Proses instalasi berlangsung

5. Setelah iSafer terinstal, Anda dapat mengklik **Finish** untuk menyudahi proses instalasi tersebut.



Gambar 1.18 Finish untuk menyudahi proses instalasi

Setelah terinstal, iSafer akan otomatis teraktifkan tiap kali Windows dijalankan, atau Anda bisa menjalankannya dari Start Screen. Berikut ini contoh penggunaan iSafer untuk firewall:

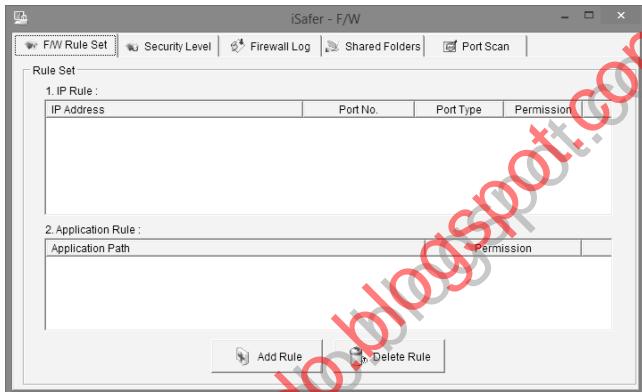
1. Ketika aktif, ada sebuah bilah yang mengandung tiga button, yaitu **Start**, **Option**, dan **Lock Screen**.



Gambar 1.19 Tampilan iSafer ketika sudah berjalan

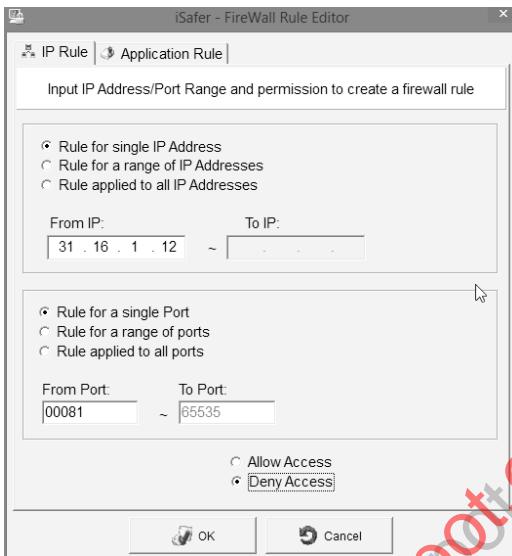
2. Button **Start** berguna menyalakan firewall.

3. Button **Options** berguna membuka window untuk mengatur opsi-opsi dari iSafer. Window **Options** di iSafer terdiri dari berbagai tab yang mengakomodasi fungsinya sendiri-sendiri. Tab yang ada antara lain **F/W Rule Set**, **Security Level**, **Firewall Log**, **Shared Folders**, dan **Port Scan**.
4. **F/W Rule** digunakan untuk mengatur rule-rule yang akan difilter oleh firewall. Keunggulan aplikasi ini adalah Anda bisa memfilter rule berdasar IP ataupun rule aplikasi. Jadi, Anda tidak hanya dapat menghalangi transfer data dari IP address, namun juga menonaktifkan aplikasi.



Gambar 1.20 Tab F/W rule untuk mengatur rule-rule di firewall

5. Untuk **IP Rule**, Anda bisa menentukan IP yang akan diatur oleh rule tersebut. ada 3 macam IP Rule, yaitu untuk IP address tunggal (**Rule for single IP Address**), yang kedua untuk IP address jangkauan (**Rule for a range of IP Addresses**), dan yang ketiga adalah semua IP address (**Rule applied to all IP Addresses**).
6. Kemudian, untuk tiap IP address yang dipilih, Anda juga dapat menentukan port-port tertentu atau semuanya. Ada 3 konfigurasi port yang bisa diatur, pertama satu port (**Rule for a single Port**), yang kedua adalah jangkauan port (**Rule for a range of ports**), dan yang ketiga semua port (**Rule applied to all ports**).



Gambar 1.21 Pengaturan IP Rule untuk F/W Rule

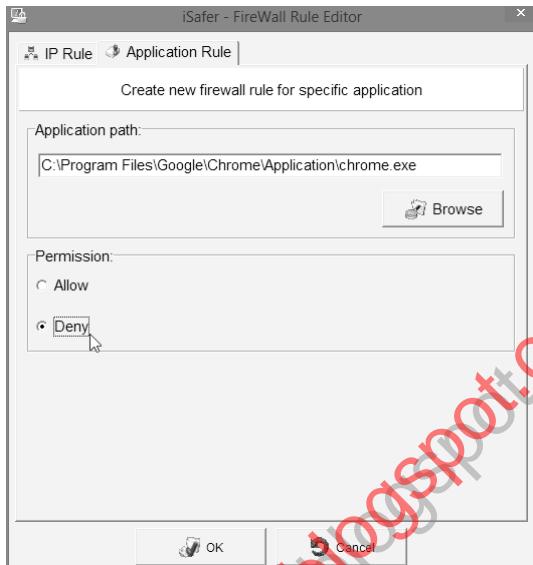
- Set juga perilaku yang diinginkan untuk rule tersebut, yaitu mengizinkan akses (**Allow Access**) atau menolak akses (**Deny Access**). Klik button OK, maka Anda mendapatkan konfirmasi apakah benar-benar ingin menambahkan rule atau tidak? Jika ingin memasukkan, klik Yes.



Gambar 1.22 Memasukkan rule ke dalam F/W rule

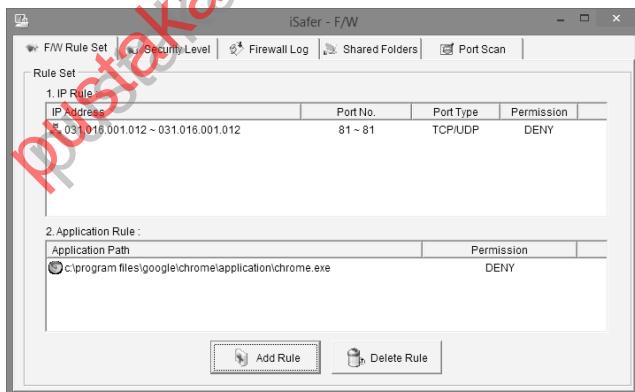
- Selanjutnya, Anda juga dapat memasukkan **Application Rule**, tempat Anda bisa membuat rule firewall untuk aplikasi tertentu. Klik pada tab **Application Rule**, kemudian klik **Browse** dan pilih file executable yang ingin dimasukkan ke dalam rule aplikasi.

9. Anda bisa menentukan permission untuk aplikasi tersebut, apakah diizinkan (**Allow**) atau ditolak (**Deny**). Klik button **OK** untuk menerapkannya.



Gambar 1.23 Pembuatan Application rule

10. Rule-rule yang sudah dimasukkan, baik IP Rule ataupun Application Rule akan diperlihatkan di tab F/W Rule Set seperti gambar berikut.



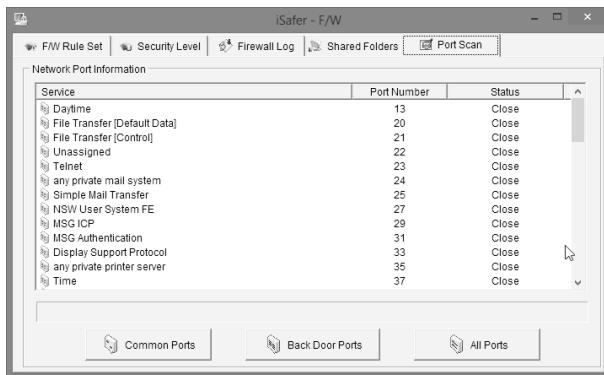
Gambar 1.24 Tampilan rule set yang mengandung rule-rule yang sudah dibuat

11. Tab **Security Level** berguna menentukan level pengamanan yang Anda inginkan. Ada 3 level pengamanan, standar adalah **Medium**, yang paling ketat adalah **High**, sementara yang rendah adalah **Low**.



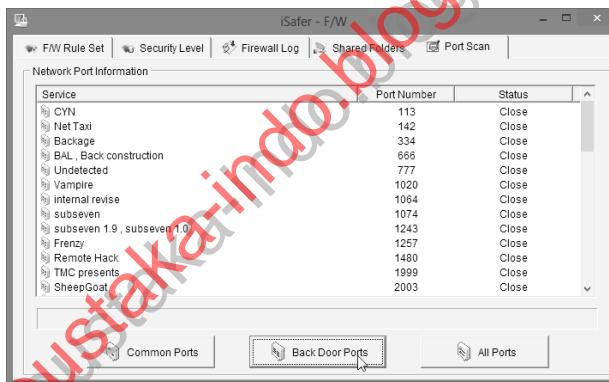
Gambar 1.25 Pengaturan security level

12. Di tab **Firewall Log**, Anda bisa melihat lalu-lintas data di komputer Anda. Anda bisa mengetahui arah lalu-lintas apakah masuk (IN) atau keluar (OUT). Anda juga bisa mengetahui alamat IP tujuan/dan hostname-nya jika ada, beserta port yang diakses atau dibuka.
13. Tab **Shared Folders** menampilkan folder-folder yang ada di komputer Anda, termasuk printer atau peranti lain, yang di-share. Anda bisa memilih untuk menghentikan sharing dengan mengklik button **Unshare**, **Open** untuk membuka folder sharing, dan **Properties** untuk melihat properti sharing dari folder yang bersangkutan.
14. Tab **Port Scan** mengenumerasi semua port yang ada di komputer. Semua port yang terbuka atau tertutup akan ditampilkan di sini. Ini membantu admin untuk mengetahui port-port mana saja yang masih terbuka, sehingga perlu ditutup demi keamanan.



Gambar 1.26 Port komputer di tab Port Scan

15. Jika button **Back Door Ports** diklik, maka yang ditampilkan hanya port-port yang memiliki kemungkinan sebagai backdoor yang biasa digunakan untuk spyware atau malware. Sementara, jika button **Common Ports** diklik, maka yang ditampilkan adalah port-port umum di komputer.



Gambar 1.27 Klik Back Door Ports

16. Untuk menghentikan firewall, klik pada button **Exit** (silang) di kanan atas. Maka, muncul tulisan status **Firewall is stopped** seperti berikut.

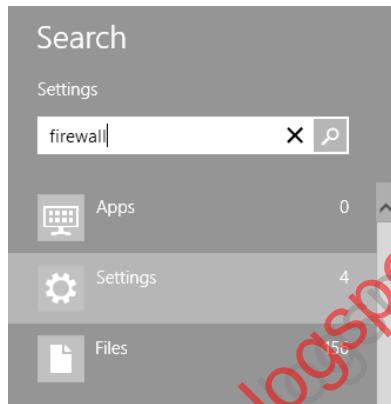


Gambar 1.28 Konfirmasi menghentikan layanan firewall

## 1.3 Windows Firewall

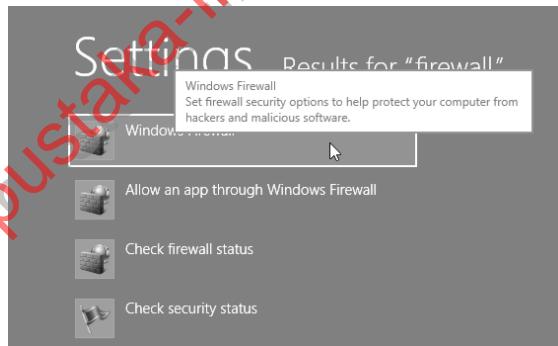
Windows Firewall adalah bawaan Windows yang menangani urusan firewall. Cara mengaktifkan dan mendefinisikan rule dari firewall Windows seperti berikut ini:

1. Tekan **Windows + F**, kemudian isikan “firewall” dan klik **Settings**.



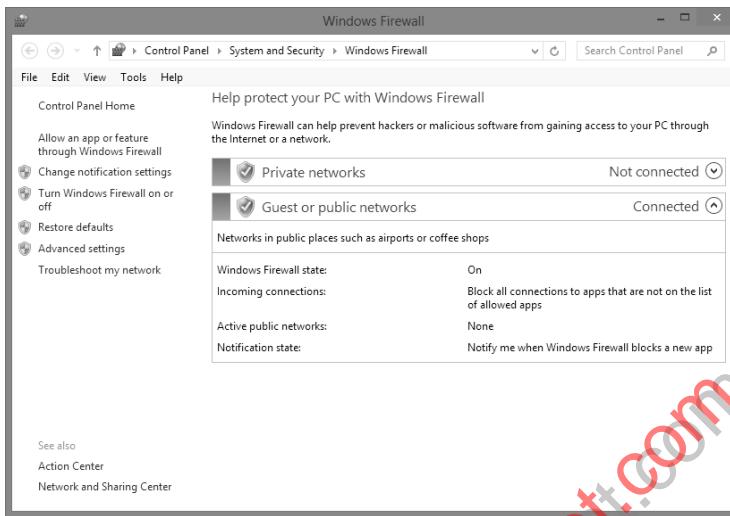
*Gambar 1.29 Klik Firewall di Search bar*

2. Muncul pilihan **Settings**, klik pada **Windows Firewall** untuk mengaktifkan Windows Firewall.



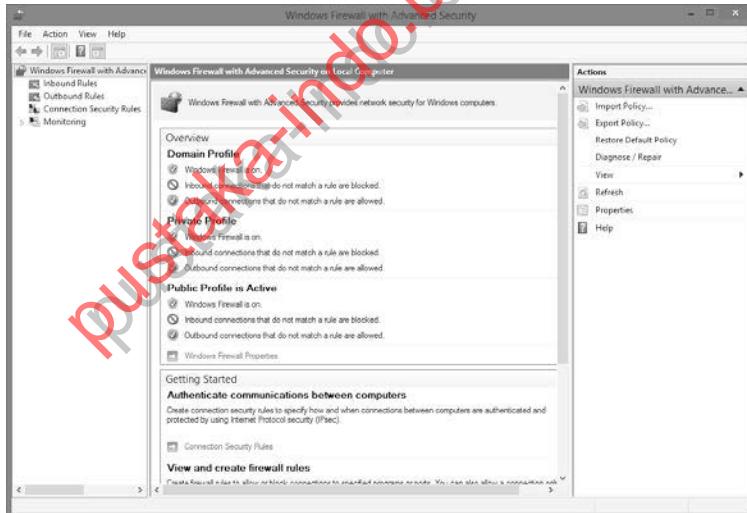
*Gambar 1.30 Klik Windows Firewall*

3. Muncul halaman pengaturan Windows Firewall seperti berikut.



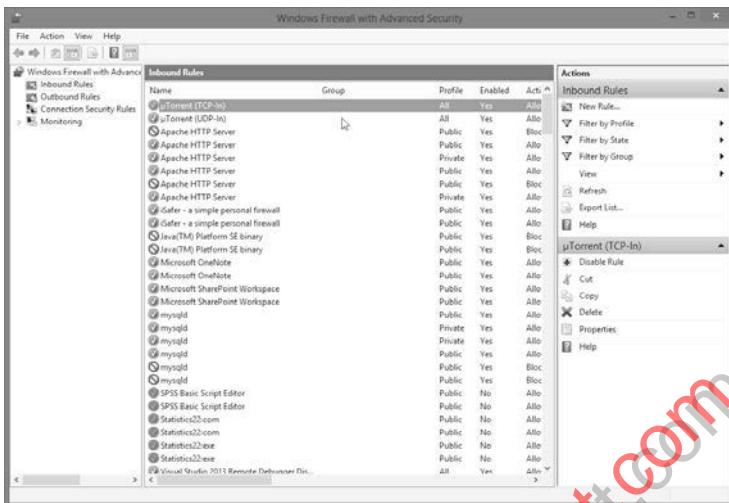
Gambar 1.31 Jendela Windows Firewall

4. Klik **Advanced Settings** untuk mengatur setting firewall lebih lanjut. Muncul jendela **Windows Firewall with Advanced security**.



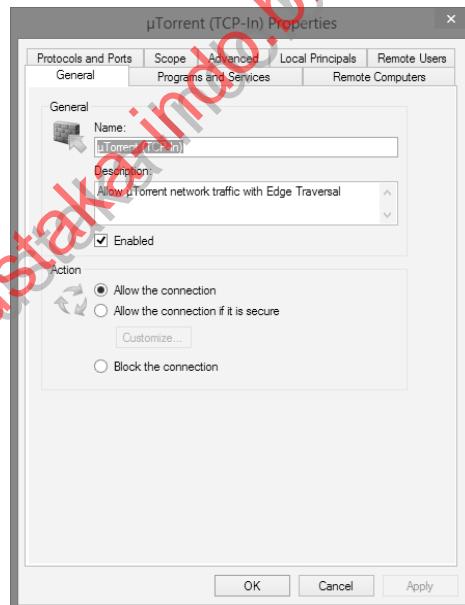
Gambar 1.32 Tampilan Advanced security di Windows Firewall

5. Klik pada **Inbound rules** untuk membuat rule inbound.



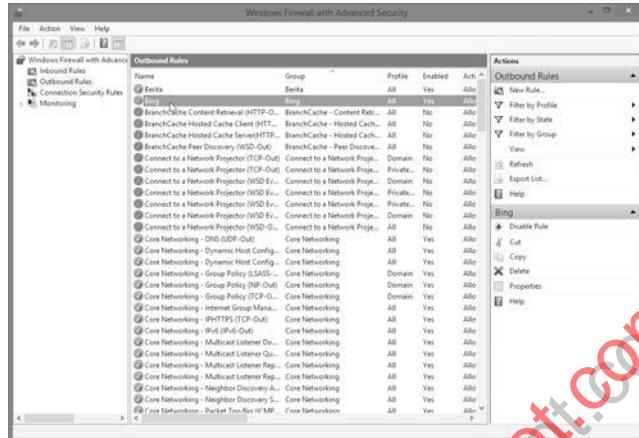
Gambar 1.33 Inbound rules untuk membuat rule inbound

6. Di sini, Anda bisa membuat atau mengedit rule inbound dari aplikasi tertentu, caranya klik pada aplikasi tersebut, lalu Anda bisa mengganti action apakah Allow atau Block.



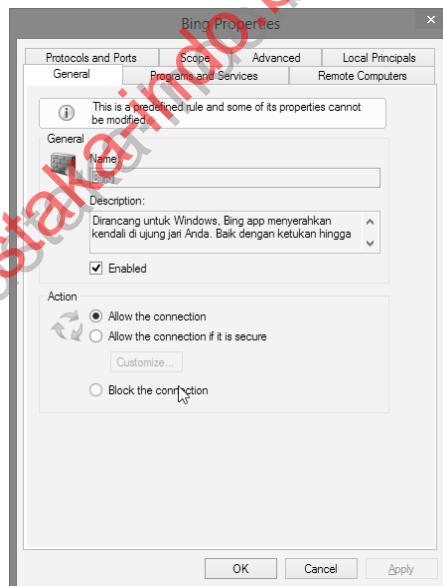
Gambar 1.34 Allow atau block connection untuk inbound application

7. Untuk outbound rule, Anda juga bisa klik pada aplikasi untuk mengedit rule outbound.



Gambar 1.35 Pengeditan rule outbound

8. Anda juga bisa mengeset apakah Enabled atau Disabled, serta menentukan jenis action, apakah membolehkan atau tidak membolehkan.



Gambar 1.36 Penentuan action outbound

[pustaka-indo.blogspot.com](http://pustaka-indo.blogspot.com)

## BAB 2

# Pengamanan AntiVirus

Saat ini, Anda pasti sering mendengar istilah “*information is power*”. Pihak yang mengetahui dan menguasai informasi di saat yang tepat, maka ialah yang menjadi pemenang. Kalimat tersebut merupakan kalimat yang sangat tepat. Informasi yang diintegrasikan, dianalisis, dan disintesis dengan benar akan memunculkan pengetahuan dan pengambilan keputusan yang benar.

Saat ini, kebanyakan informasi yang ada di dunia disimpan atau diolah dari sumber informasi digital dan kebanyakan di komputer. Informasi-informasi dalam bentuk digital lebih mudah diambil dan ditransfer ke sistem lain dibandingkan informasi yang disimpan dalam bentuk konvensional.

Betapa banyak keputusan yang kritis diputuskan dan dieksekusi berdasarkan data yang diambil dalam bentuk digital. Ini menunjukkan bahwa melindungi informasi digital sangat penting peranannya. Sering sudah kita mendengar, bahwa informasi-informasi penting -seperti kemiliteran- bocor ke media massa karena kecerobohan pekerja militer yang tak pandai menyimpan dan menjaga akurasi data.

Intinya, agar sebuah informasi benar-benar bisa menjadi “power”, Anda perlu menjaga informasi tersebut agar tetap akurat, benar, dan bisa diakses tepat waktu. Selain itu, informasi tersebut juga harus bisa dipertukarkan atau diakses dari sistem lain dengan aman dan handal. Salah satu aspek untuk menjaga informasi tetap benar adalah menggunakan antivirus.

Antivirus adalah program yang bisa digunakan untuk menjaga virus dari komputer Anda. Selain itu, antivirus juga bisa digunakan untuk mematikan virus saat virus sudah terlanjur aktif di komputer.

Saat ini antivirus sudah merupakan produk yang banyak digunakan di komputer, terutama di komputer Windows. Di komputer Linux pun, antivirus tetap diperlukan. Antivirus sudah memiliki berbagai versi, baik komersial ataupun open source.

Untuk melindungi komputer, program antivirus umumnya menggunakan dua teknik. Pertama adalah menggunakan signature, yaitu gambaran sekilas dari pola kode virus. Program antivirus akan berjalan di background mengawasi file atau program yang berjalan di komputer. Jika antivirus mendeteksi adanya pola yang sesuai dengan signature yang dimilikinya, maka antivirus akan memberitahukan bahwa antivirus mendeteksi ada pola yang mirip dengan yang di database-nya, atau dengan kata lain antivirus menjumpai file yang merupakan “tersangka virus”.

Selain pasif seperti di atas, antivirus juga bisa melakukan pendekatan yang aktif. Yaitu, antivirus akan memindai harddisk dan memory komputer serta mendeteksi dan melaporkan jika ada kode, file, atau program yang mencurigakan, lalu menempatkan program-program yang mencurigakan tersebut ke karantina.

Salah satu kekurangan dari antivirus yang menggunakan signature adalah perlunya update signature-signature virus terbaru secara kontinyu agar antivirus tersebut bisa efektif lantaran mengenali virus-virus yang terbaru. Karena sudah barang tentu virus-virus selalu berkembang dan karenanya antivirus yang tidak mengenali virus terbaru ibaratnya menjadi macan ompong.

Cara untuk meng-update signature virus yang paling lazim adalah via WWW. Baik download melalui internet secara manual, atau otomatis melalui fasilitas autoupdate dari software antivirus yang bersangkutan.

Semakin lama, tentu jumlah virus semakin besar, karena itu jumlah file yang perlu Anda update akan semakin banyak pula. Selain itu, intensitasnya akan bertambah.

Masalah lain dari teknik signature ini adalah kemampuan virus untuk memutasi dan berubah bentuk atau polimorfisme. Beberapa programmer menggunakan software kompresi file yang memungkinkan signature dari virus tidak terdeteksi ketika tidak aktif.

Untuk menangani kekurangan-kekurangan di atas, produsen antivirus menambahkan teknik kedua untuk mendeteksi virus, yaitu teknik deteksi heuristik. Teknik heuristik pada dasarnya adalah sebuah aturan atau perilaku tertentu. Jika sebuah program memiliki perilaku yang sesuai dengan ciri-ciri virus, maka software akan otomatis berusaha untuk menghentikannya. Misalnya sebuah program yang tiba-tiba ingin mengakses bagian kritis dari sistem operasi, maka antivirus akan otomatis menghentikannya. Begitu pula jika ada program yang hendak mengakses sektor di harddisk yang berkaitan dengan definisi tabel di harddisk, maka otomatis antivirus akan menyetopnya.

Salah satu perilaku virus lainnya adalah perubahan ukuran file menjadi lebih besar atau lebih kecil tanpa sebab. Perubahan kapasitas hard disk secara tiba-tiba dan perubahan atribut tanggal atau waktu pembuatan file tertentu.

## 2.1 Anatomi AntiVirus

Sebuah antivirus umumnya mengandung komponen yang disebut scanner virus. Scanner virus merupakan fitur antivirus yang otomatis mendeteksi dan menyingkirkan virus sebelum virus tersebut aktif. Tujuan scanner virus adalah mendeteksi virus dan menyingkirkannya, sebelum virus tersebut menyebabkan kerusakan, seperti penghapusan file, menimpa file tertentu, menambah atau mengurangi file.

Scanner virus hampir mirip dengan software *Intrusion Detection System* (IDS). Yaitu, bekerja dengan memeriksa kode di program yang ada di sistem atau ingin memasuki sistem.

Ada 4 tipe utama scanner virus, yaitu:

- Memonitor aktivitas.

- Memonitor perubahan dan integritas.
- Scanner murni.
- Hibrida.

Memonitor aktivitas merupakan tipe paling tua dari software anti-virus. Cara kerjanya sama dengan IDS, yaitu mendeteksi adanya aktivitas dengan pola mencurigakan yang bisa mengindikasikan adanya aktivitas virus.

Teknik memonitor perubahan dan integritas akan mengecek apakah ada file yang berubah dengan mengecek checksum dari integritasnya. Teknik memonitor perubahan ini cenderung mudah error, dalam arti memiliki kecenderungan *false positive* yang tinggi, yaitu sesuatu yang bukan virus dapat disangka virus.

Scanner murni bekerja dengan cara memeriksa sistem, file user, boot sector dan memory, serta melihat apakah ada virus atau tidak. Teknik mana yang banyak dipakai oleh software antivirus? Yaitu teknik hibrida, atau gabungan dari teknik-teknik di atas.

Ketika hendak menginstal antivirus, Anda juga harus mengenal beberapa aturan best practice dalam penggunaan antivirus, di antaranya sebagai berikut:

- Jangan menggunakan antivirus sembarangan, kecuali dari pengembang antivirus yang terpercaya dan terkenal.
- Jangan men-download file ketika update signature, kecuali dari sumber yang terpercaya.
- Lakukan backup secara teratur untuk menghindari hilangnya data penting, jikalau seandainya antivirus gagal mendeteksi virus berbahaya yang merusak file dan komputer.
- Terapkan access control secara ketat, misalnya memakai kewenangan guest untuk akses komputer sehari-hari dan hanya memakai administrator saat akses kontrol sistem.
- Jangan buka attachment di email yang mencurigakan.
- Jangan membuka email yang tak dikenal dan mencurigakan, misalnya email yang memiliki header yang sama, namun dengan pengirim yang berbeda-beda.

## 2.2 Mengenal Virus

Sebelum menerapkan antivirus, pertama Anda harus mengenal apakah virus itu sebenarnya? Virus sebenarnya adalah sebuah program komputer alias software. Virus memiliki kode di dalamnya yang memungkinkan virus menyalin dirinya sendiri atau menempelkan dirinya ke program lain.

Virus juga mengandung kode yang memungkinkannya memodifikasi program. Berbeda dengan worm, virus umumnya memiliki induk semang tempat menempelkan dirinya. Saat ini, virus sudah sangat menyebar dan tingkat bahayanya pun semakin bertambah.

Virus dapat menginfeksi berbagai bagian di komputer, dari mulai memory, floppy disk, hard drive, backup tape, atau media storage lain. Yang umum sekarang adalah USB flash disk. Virus juga bisa menyebar via jaringan *Local Area Network* (LAN), internet, atau penggunaan software dan disket yang terinfeksi.

Di awal sejarahnya, umumnya virus dibuat oleh seorang yang jenius, seperti ahli komputer, dan peneliti keamanan di perusahaan atau laboratorium. Tapi, kini virus sudah lazim dikembangkan oleh seorang atau sekelompok programmer yang tidak bekerja untuk siapa-siapa. Motifnya bermacam-macam, ada yang cuma ingin numpang tenar, pamer skill programming, atau memang bertujuan jahat merusak komputer tertentu atau semua komputer tanpa pandang bulu.

Virus ada berbagai macam jenisnya, dari mulai virus yang tidak membahayakan dan hanya sekedar membebani memory atau kinerja komputer hingga yang sangat mengerikan, yaitu yang langsung merusak sistem operasi komputer, atau menghilangkan file-file tipe tertentu yang dijumpainya tanpa ampun.

Virus yang menyerang komputer juga bisa menyedot bandwidth dari koneksi internet, karena virus umumnya melakukan ping atau mendownload konten secara clandestine (diam-diam) tanpa sepengetahuan pengguna komputer. Hasilnya sangat merugikan, terutama jika pengguna komputer menggunakan koneksi internet yang non-unlimited, karena harus membayar biaya koneksi internet dengan jumlah yang sangat banyak.

Virus juga bisa diciptakan untuk mencuri data, membuat data tak stabil/corrupt, atau menjadikan komputer sebagai zombie yang bisa dikendalikan dan disadap dari jarak jauh.

Virus merupakan sebuah software yang bisa dikategorikan sebagai kuman di komputer, karena bisa menyedot sumber daya komputer, menyebarkan diri, dan mereproduksi tanpa bisa dikendalikan. Virus dapat didefinisikan menjadi beberapa kategori:

- Boot virus: Virus yang menyerang bagian boot sector dari harddisk atau floppydisk dan diaktifkan saat power-on.
- Macro virus: Virus yang diletakkan menempel pada dokumen office, biasanya software word processing atau spreadsheet sebagai macro. Jadi, program ini akan diaktifkan ketika macro dieksekusi.
- Program virus: Virus yang ditempelkan dan menyerang pada file \*.exe, \*.com, \*.sys, dan \*.dll. Virus akan menyerang ketika file .exe, .com, dan sebagainya dieksekusi atau digunakan oleh aplikasi lain.
- Transient virus: Virus yang aktif jika program yang diinfeksi dieksekusi. Jika program tidak dieksekusi, maka virus akan mematikan diri sendiri.
- Resident virus: Virus yang bertempat tinggal di memory dan me-link dirinya sendiri ke eksekusi program lain.

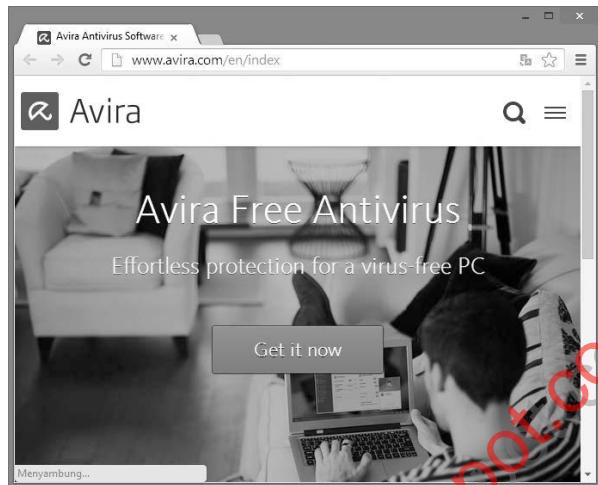
Walaupun perkiraannya bisa sangat bervariasi, namun kerugian yang dialami oleh virus terlihat nyata. Beberapa kerugian yang dialami oleh virus antara lain adalah kerugian waktu dan tenaga yang perlu dikerahkan untuk membersihkan virus dari komputer.

Kerugian software ataupun kehilangan data juga bisa berharga mahal jika data yang hilang merupakan data yang sangat penting. Karena itu menghitung jumlah kerugiannya sangat sulit, karena melibatkan faktor emosional terhadap file tersebut.

## 2.3 Avira Antivir

AntiVir adalah sebuah program antivirus yang dikembangkan oleh sebuah perusahaan dari Jerman yang bernama AntiVir GmbH.

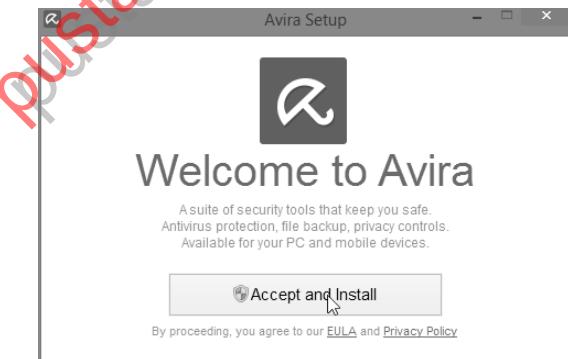
Anda bisa mendownload AntiVir ini dari berbagai sumber, antara lain via download.com di <http://avira.com>.



Gambar 2.1 Website Avira AntiVir

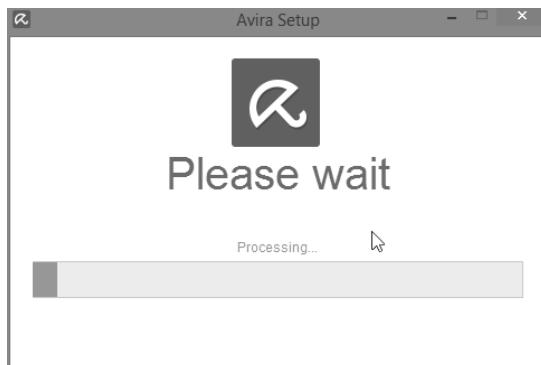
Ukuran file AntiVir cukup besar, saat buku ini ditulis, versi terbarunya sudah berukuran 21 MB. Karena itu saat download, usahakan menggunakan software download client, misalnya Free Download Manager atau DownThemAll (plugin dari Firefox). Setelah terdownload, instal dahulu dengan cara berikut:

1. Eksekusi file installer AntiVir, jendela pertama yang muncul terlihat seperti di bawah. Klik **Accept and Install** untuk mulai menginstal aplikasi AntiVir ini.



Gambar 2.2 Jendela instalasi Avira AntiVir

2. Maka muncul aplikasi untuk ekstraksi dan instalasi aplikasi.



Gambar 2.3 Ekstraksi file installer AntiVir

3. Tunggu hingga tahapan proses download selesai. Proses ini cukup memakan waktu lama, kecepatannya tergantung kepada koneksi internet Anda, ukurani filenya sekitar 130-an MB.



Gambar 2.4 Proses download

4. Kalau sudah terinstal, maka di bagian Antivirus memiliki tulisan **Malware protection**.



Gambar 2.5 Tulisan malware protection

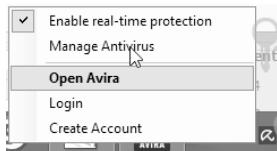
5. Memulai pemindaian pertama, klik **Scan**.



Gambar 2.6 Klik Scan untuk pemindaian pertama

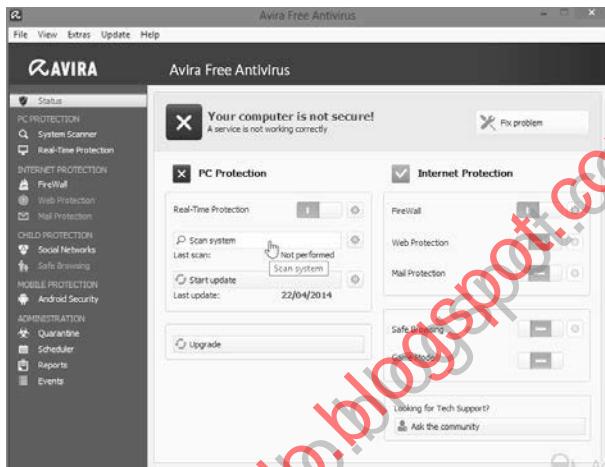
Apabila AntiVir sudah terinstal, selanjutnya Anda tinggal mengaktifkan AntiVir dengan menggunakan Start screen atau klik kanan di Notification Area. Berikut ini cara mengoperasikan Antivir:

1. Klik kanan, kemudian klik menu **Open Avira**.



Gambar 2.7 Klik kanan dan pilih menu Open Avira

2. Kemudian, klik pada link **Scan system** untuk scan PC.



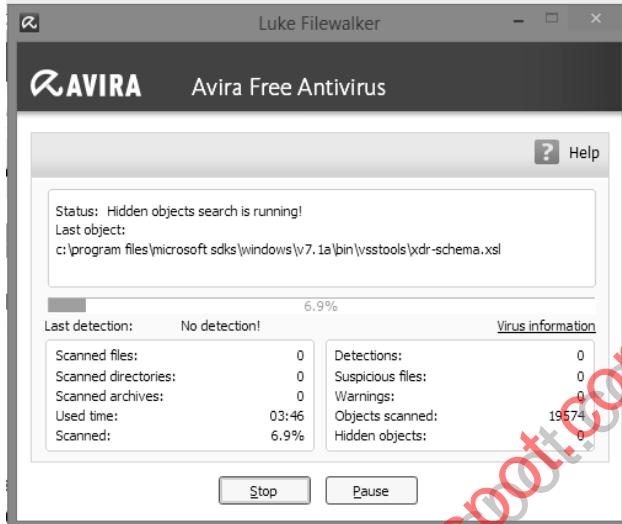
Gambar 2.8 Klik pada Scan system

3. Muncul jendela Luke Filewalker di mana file Anda sedang dipindai oleh Avira Antivir.



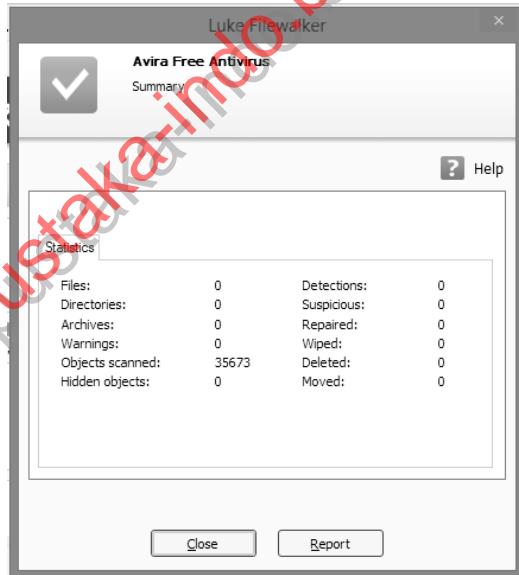
Gambar 2.9 File sedang dipindai

4. Tunggu hingga proses pemindaian ini selesai.



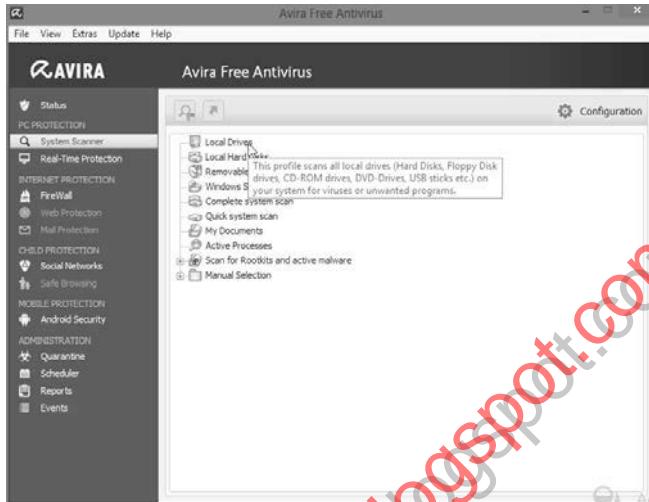
Gambar 2.10 Proses pemindaian sedang berlangsung

5. Hasilnya muncul di Avira Free Antivirus Summary.



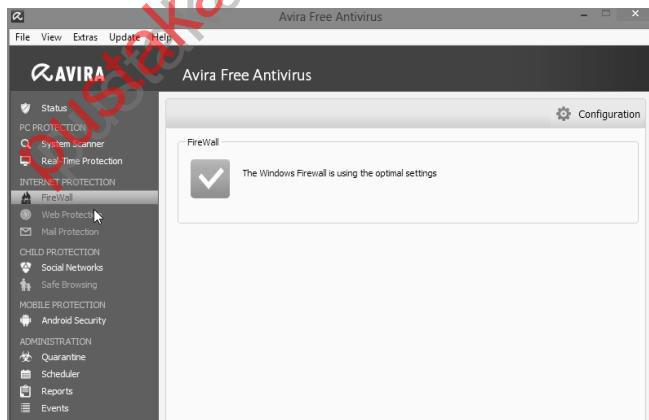
Gambar 2.11 Hasil pemindaian

6. Buka jendela **Avira Free Antivirus**, Anda dapat melihat banyak pengaturan di sini. Di **PC protection > System scanner**, Anda bisa melihat berbagai komponen file dari **Avira Free AV** yang bisa dipindai.



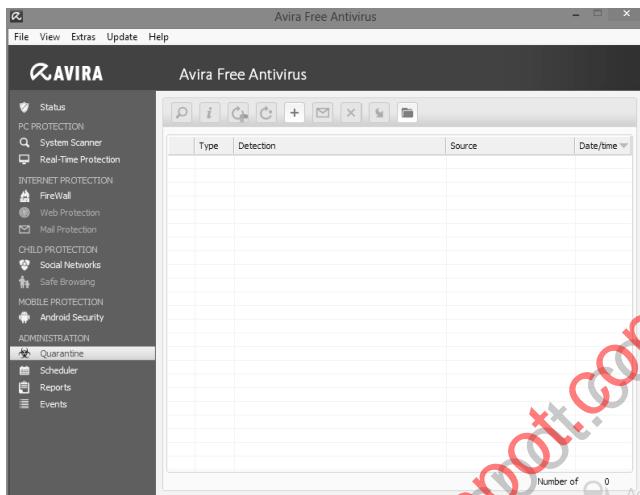
Gambar 2.12 Jendela Avira Free AV

7. Di **Internet Protection > Firewall**, Anda bisa melihat status firewall di komputer, kalau misalnya Windows Firewall atau software firewall lain sudah terpasang, Anda bisa melihat status pengoperasian firewall tersebut.



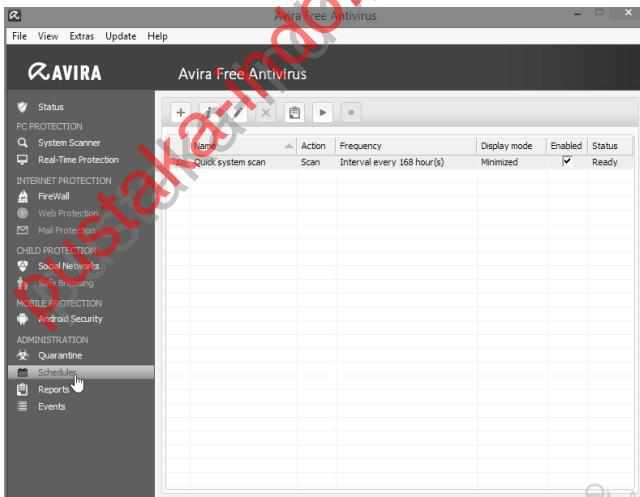
Gambar 2.13 Status operasi firewall

8. Di **Quarantine**, Anda bisa melihat apakah ada file virus atau malware yang dikarantina atau tidak?



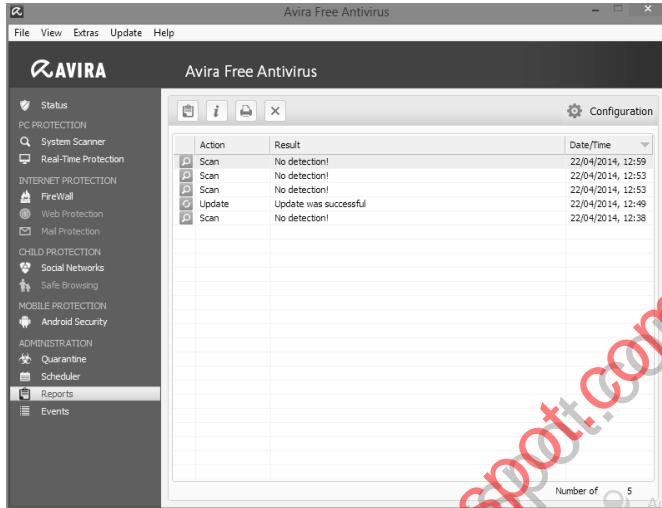
Gambar 2.14 Quarantine

9. Di **Schedule**, Anda bisa melihat daftar apakah ada pemindaian yang terjadwal atau tidak.



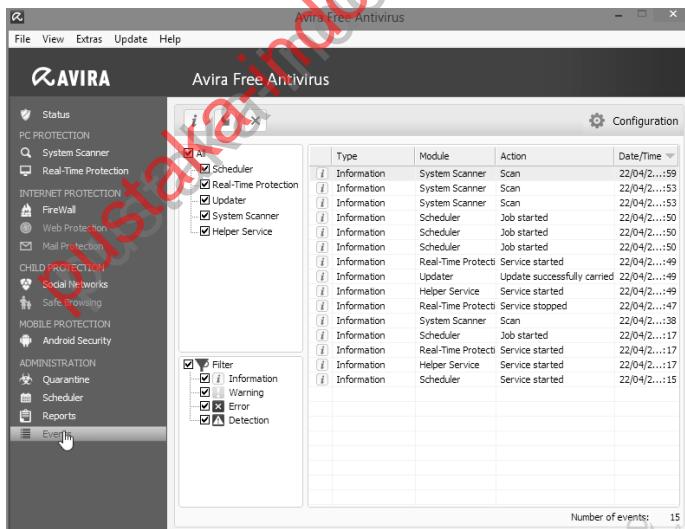
Gambar 2.15 Jadwal Scheduled maintenance

10. Di **Reports**, Anda bisa melihat laporan-laporan dari aplikasi antivirus ini.



Gambar 2.16 Laporan dari program anti virus

11. Di **Events**, terlihat catatan event yang berkaitan dengan program Avira Antivir ini.

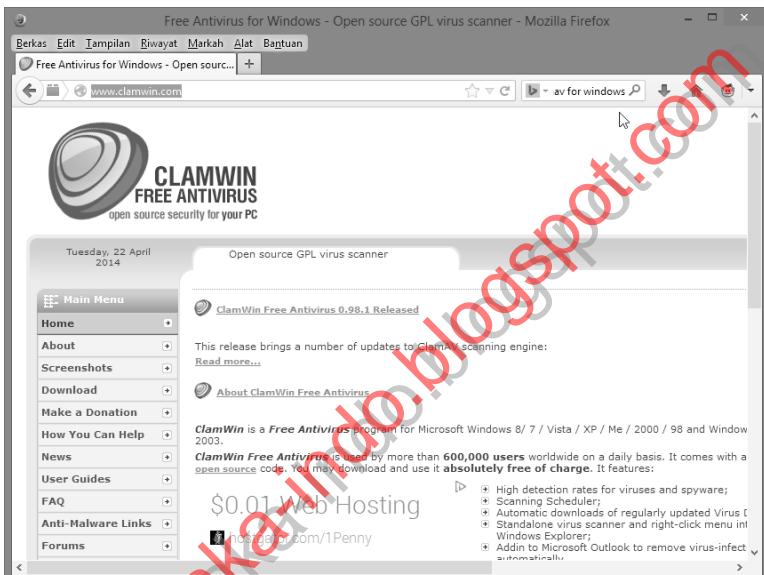


Gambar 2.17 Catatan Events Avira Antivir

## 2.4 ClamWin

ClamWin merupakan salah satu dari banyak varian antivirus ClamAV (aslinya berjalan di platform Unix/Linux) yang di-porting ke Windows.

Software ini didukung oleh lisensi GPL versi 2. Artinya, software ini bebas untuk diunduh dan diperoleh dengan gratis, kode sumbernya pun terbuka dan bebas diutak-atik. Software ini bisa di-download dari [www.clamwin.com](http://www.clamwin.com).



Gambar 2.18 Situs untuk download clamav di [clamwin.net](http://clamwin.net)

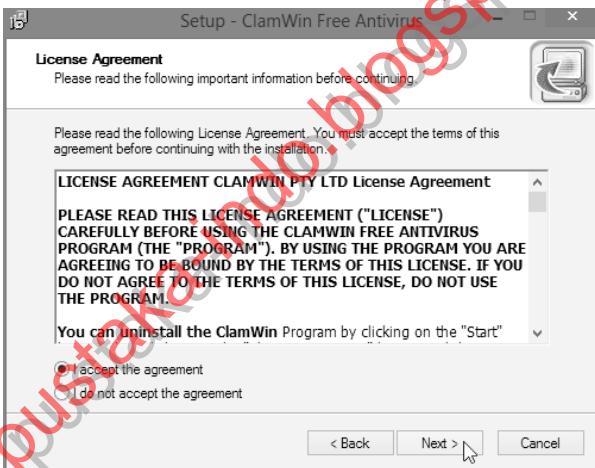
Setelah download, Anda dapat menginstal terlebih dahulu ClamWIn FreeAV ini dengan cara seperti berikut:

1. Eksekusi file installer yang sudah di-download. Pertama kali, muncul jendela **Welcome to the ClamWin Free AV Setup Wizard**, klik **Next**.



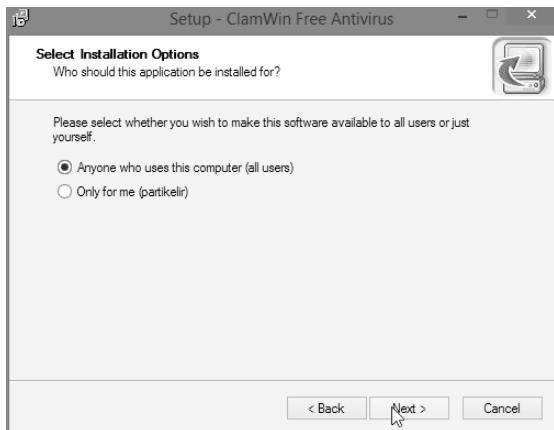
Gambar 2.19 Jendela Welcome to the License Agreement

2. Muncul jendela lisensi di License Agreement, klik Next.



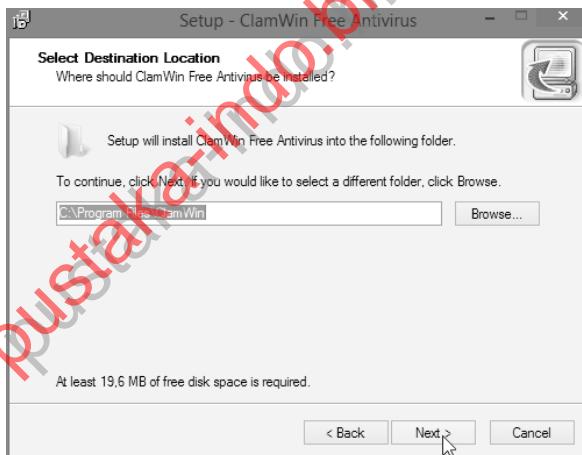
Gambar 2.20 Lisensi ClamAV

3. Muncul Select installation options, pilih opsi instalasi yang Anda inginkan, apakah akan diinstal ke semua user komputer, atau hanya username tertentu saja.



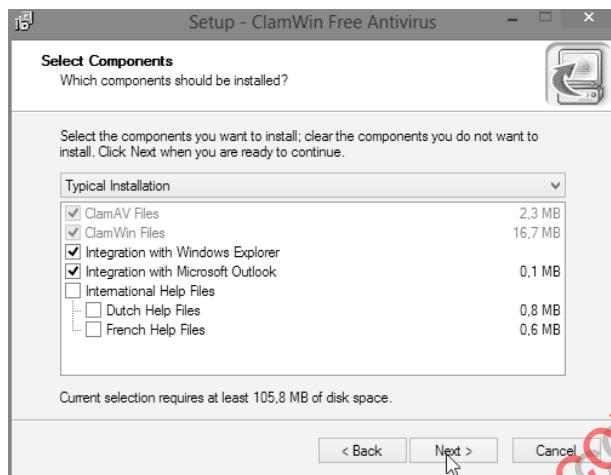
Gambar 2.21 Penentuan opsi instalasi

4. Berikan lokasi untuk instalasi ClamWin. Dalam kondisi default, lokasinya adalah C:\Program Files\ClamWin dan klik button **Install**. Jika hendak mengubah, klik button **Browse** dan pilih folder baru di kotak yang muncul. Jika sudah, klik button **Install**.



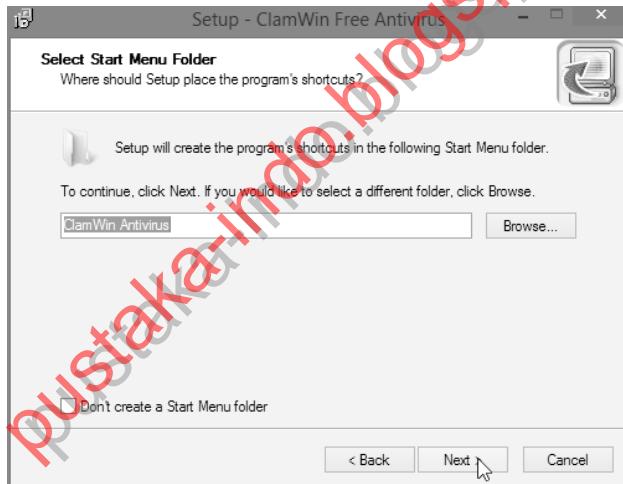
Gambar 2.22 Penentuan folder instalasi

5. Pilih komponen di **Select Components**, kalau menggunakan Explorer dan Mail client, cek pada **Integration with Windows Explorer** dan **Integration with MS Outlook**.



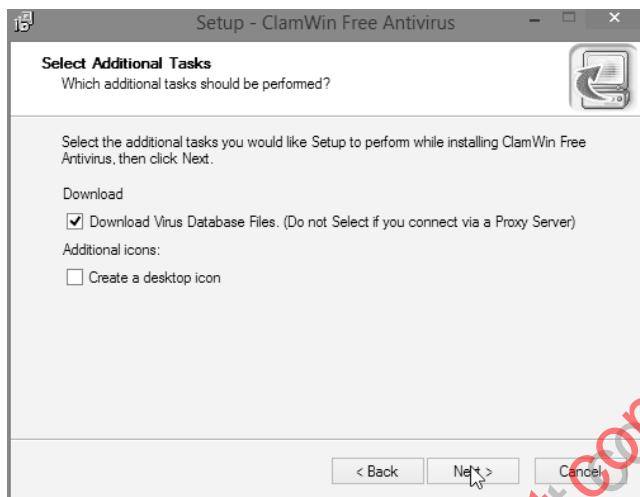
Gambar 2.23 Pilihan di Select Components

6. Tentukan nama folder untuk start menu, dan klik Next.



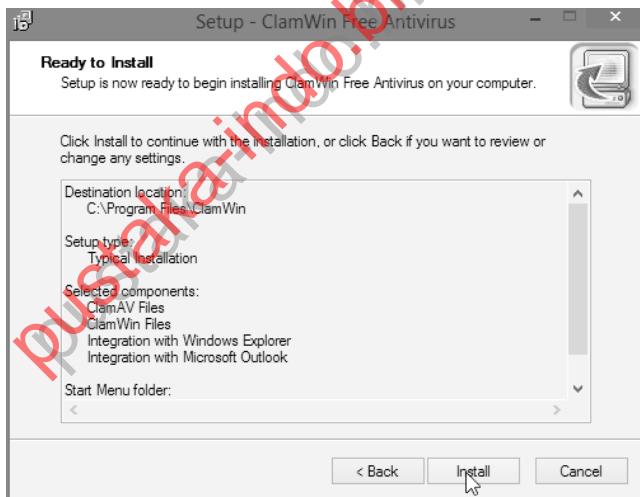
Gambar 2.24 Penentuan nama start menu folder

7. Di **Select additional tasks**, Anda bisa klik **Download Virus Database Files** agar kemampuan mengenali virus lebih baik, karena definisi virus terus dimutakhirkan.



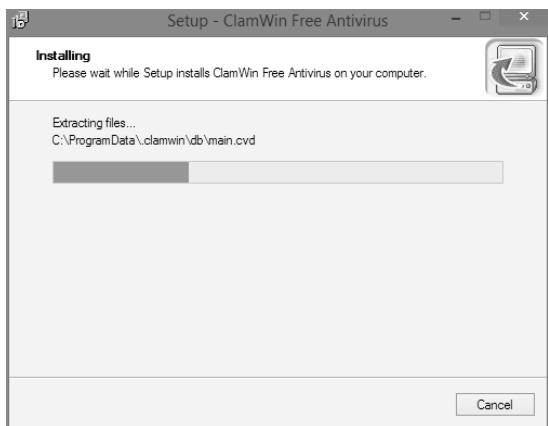
Gambar 2.25 Pilihan di Select additional tasks

8. Kalau sudah siap menginstal, rekap instalasi ditampilkan di jendela **Ready to Install**. Klik **Install** untuk memulai menginstal.



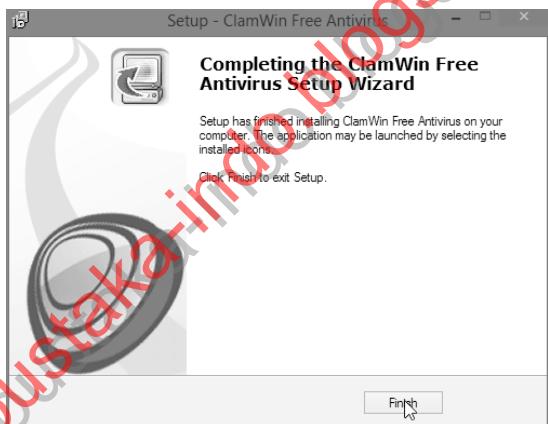
Gambar 2.26 Ringkasan di Ready To Install

9. Tunggu hingga proses instalasi selesai berlangsung.



Gambar 2.27 Proses instalasi selesai berlangsung

10. Kalau sudah terinstal dengan baik, akan muncul jendela **Completing the ClamWIN Free AV Setup Wizard**. Klik **Finish**.

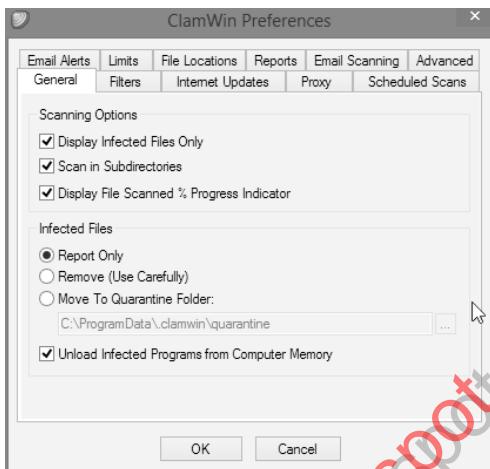


Gambar 2.28 Instalasi ClamWinFree AV selesai

Untuk menggunakan ClamWin, caranya seperti berikut ini:

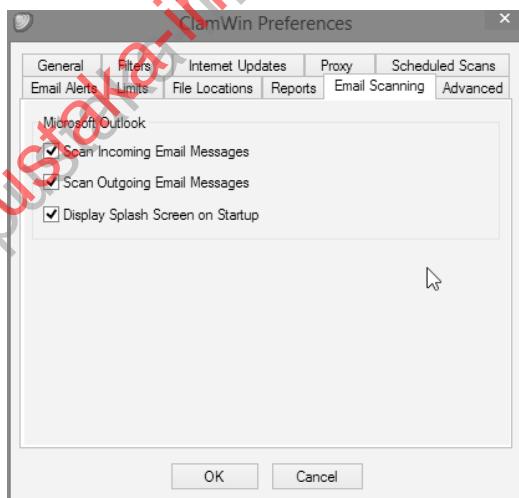
1. Klik kanan dan pilih **Configure ClamWin**.
2. Muncul jendela pengaturan ClamWin. Di tab **General**, Anda bisa menentukan opsi pemindaian, apakah akan memindai file yang terinfeksi saja, subdirektori, dan apakah akan menampilkan persentase kemajuan pemindaian.

3. Anda juga dapat menentukan perlakuan terhadap file yang terinfeksi, apakah dilaporkan saja, di-remove, atau dipindahkan ke folder karantina.



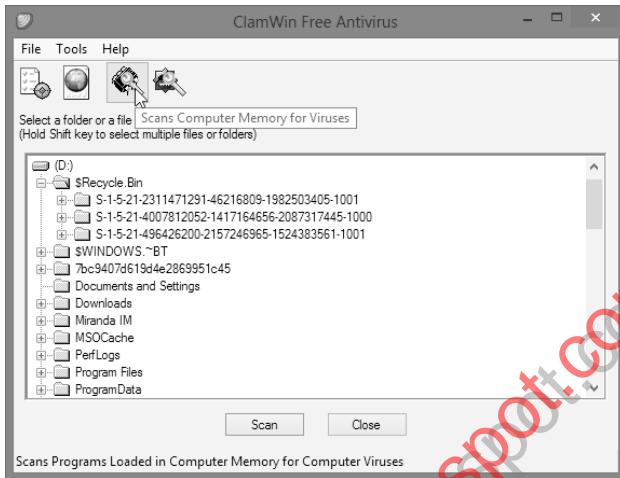
Gambar 2.29 Tab General di ClamWin Preferences

4. Di **Email Scanning**, Anda bisa memindai email dari aplikasi Mail Client Anda. Anda bisa menentukan bagian apa saja yang dipindai, apakah pesan email masuk, dan pesan email keluar.



Gambar 2.30 Pemindaian email masuk dan keluar

5. Untuk memulai memindai pada lokasi tertentu, buka ClamWin Free AV, kemudian pindai folder yang diinginkan, dan klik tombol **Scan computer memory for viruses**.



Ganbar 2.31 Jendela utama ClamWin AV

## BAB 3

# Menghindari Ancaman Online

Internet sudah jadi barang yang jamak di kehidupan kita. Ketika berbincang tentang internet, kebanyakan orang mengira bahwa yang dimaksud internet hanyalah browsing di World Wide Web atau WWW.

Padahal, sebenarnya WWW hanyalah sebagian kecil saja dari layanan internet. Bahkan sesungguhnya internet terdiri dari berbagai skema komunikasi yang disebut sebagai protokol.

Semua protokol tersebut memiliki kesamaan, yaitu ditransmisikan oleh sistem yang sama. Yaitu, sistem berbasis paket yang disebut *Transmission Control Protocol/Internet Protocol* atau lebih sering disingkat sebagai TCP/IP.

Ada banyak protokol yang menyusun internet. Hampir semua protokol ini merupakan public domain yang bersifat terbuka dan tidak bersifat komersil. Sehingga, tidak ada satu pihak pun yang bisa mengkomersialisasikan internet atau menguasai internet.

### **3.1 File Transfer Protocol (FTP)**

File Transfer Protocol berguna untuk memungkinkan transfer data secara cepat dan handal antara sebuah tempat penyimpanan file yang disebut FTP server dan komputer yang menggunakan software klien FTP yang disebut FTP Client.

Jadi dengan menggunakan FTP, user dapat menyalin file antara komputer lokal dengan sistem lain yang tergabung di jaringan internet, walaupun menggunakan platform yang berlainan, asalkan mendukung protokol FTP. FTP memiliki banyak implementasi dan protokol ini paling banyak digunakan sebagai metode bagi user untuk mentransfer file dan mengaturnya secara remote.

FTP menggunakan 2 protokol sekaligus, yaitu Telnet dan TCP. Sifat FTP adalah full duplex, artinya satu channel dapat digunakan untuk mentransmisikan data secara dua arah pada satu waktu yang sama. FTP memiliki karakteristik khusus, seperti:

- Multi fungsi: FTP dapat menangani transfer file untuk banyak tujuan.
- Tipe file bebas: FTP dapat mentransfer file data apa pun secara bebas, Anda dapat mentransfer file gambar, video, teks, file yang bisa dieksekusi (executable), dan lainnya.
- Autentifikasi dan kepemilikan: FTP memungkinkan file memiliki kepemilikan dan batasan akses.
- Mengakomodasi keragaman: FTP menyembunyikan detail dari sistem komputer tempat FTP server atau client tersebut berada.

FTP merupakan protokol yang cukup tua yang masih digunakan di internet sekarang. Bahkan diciptakan lebih dahulu dibandingkan protokol TCP ataupun IP. Namun setelah TCP/IP diciptakan, versi baru dari FTP pun dirilis untuk menyesuaikan dengan protokol TCP/IP yang baru tersebut.

Di awal munculnya internet, FTP masih lebih banyak digunakan dibandingkan transfer web. Hingga mulai tahun 1995, transfer web mulai lebih banyak traffic-nya dibandingkan web. FTP memiliki banyak perintah di dalamnya, ada lagi perintah tambahan tergantung kepada server FTP yang digunakan. Berikut ini beberapa perintah-perintah standar yang ada di protokol FTP.

!	cr	macdef	proxy	sendport
\$	delete	mdelete	put	status
account	debug	mdir	pwd	struct
append	dir	mget	quit	sunique
ascii	disconnect	mkdir	quote	tenex
bell	form	mls	recv	trace
binary	get	mode	remotehelp	type
bye	glob	mput	rename	user
case	hash	nmap	reset	verbose
cd	help	ntrans	rmdir	?
cdup	lcd	open	runique	
close	ls	prompt	send	

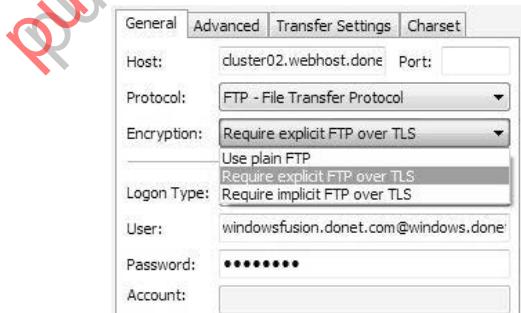
### **Gambar 3.1 Perintah-perintah FTP**

Ada 2 mesin yang diperlukan dalam sebuah transaksi FTP, yaitu mesin client atau biasa disebut *local host* dan mesin server yang disebut *remote host*. Dari kedua mesin tersebut, yang pertama kali memulai transfer adalah client. Perintah *get* digunakan untuk menyalin file dari server ke client, sementara perintah *put* digunakan untuk menyalin file dari client ke server.

Spesifikasi FTP, awalnya bukanlah spesifikasi yang aman dalam mentransfer data. Karena tidak ada metode khusus untuk mentransfer data dalam mode terenkripsi. Artinya, informasi penting seperti username, password, command FTP, dan file yang ditransfer bisa dikuping oleh orang lain di jaringan menggunakan software yang disebut *packet sniffer*. Ini juga sebenarnya masalah yang sama yang dihadapi oleh semua protokol internet yang ditulis sebelum diciptakannya SSL.

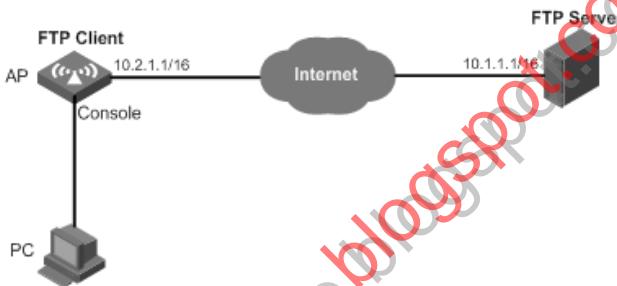
Karena itu, ada 3 prinsip mengamankan transfer FTP:

- Jika server mendukung, usahakan terkoneksi ke server menggunakan enkripsi, seperti SFTP (*SSH File Transfer Protocol*). Yaitu, fitur yang menambahkan enkripsi SSL atau TLS ke FTP.



**Gambar 3.2 Pemilihan mode enkripsi di FTP client**

- Gunakan prinsip security user normal, yaitu dengan menggunakan password dan username. Server harus mengalokasikan untuk tiap orang berupa username dan password yang kuat. Username dan password tersebut nantinya digunakan untuk mengakses server FTP.
- Konfigurasikan sistem dengan benar. Misalnya, FTP server harus dijalankan di sistem operasi yang modern, seperti Windows Server atau Linux/Unix yang teruji kredibilitasnya. Pastikan, software FTP server atau FTP client yang digunakan merupakan versi yang terbaru. Jumlah port yang digunakan harus minimal, namun masih tidak mengganggu proses transfer.



*Gambar 3.3 Cara kerja koneksi FTP*

Selain itu, dari sisi FTP server, ada beberapa prinsip pengamanan yang harus diterapkan, yaitu:

- Matikan akses anonymous: Akses anonim umumnya diizinkan secara default ketika FTP server diinstal. Akses anonim adalah sebuah metode yang mengizinkan user untuk mendapatkan akses ke situs FTP tanpa memiliki account user.

Walaupun fitur ini secara asli diaktifkan, namun bisa menimbulkan masalah karena orang bisa membajak server FTP Anda secara ilegal. Karena itu, matikan saja akses anonim untuk mengamankan FTP server.

Dengan demikian, hanya user yang berwenang saja dan terotentifikasi oleh username dan password yang bisa mengakses FTP server.

- Aktifkan pencatatan log: Dengan mengaktifkan pencatatan log di server FTP, Anda akan memperoleh catatan akurat tentang IP dari pengakses dan apa yang diakses oleh user. Dengan menerapkan pencatatan log, Anda dapat mengakses pola lalu-lintas data dan mengenali apabila ada ancaman terhadap server FTP.
- Terapkan kewenangan secara ketat: Pengaksesan direktori FTP haruslah diatur secara ketat. Misalnya, Anda bisa mengeset agar user dapat mentransfer file ke server, namun tidak bisa membaca isi file yang ada di server. Implementasinya adalah, user diberi kewenangan untuk **Write** dan **Log Visits**, namun tidak memiliki log **Read**.
- Aktifkan kuota disk: Beberapa sistem operasi seperti Windows Server memungkinkan adanya pengaturan kuota disk. Kuota disk dapat menghalangi seorang untuk mentransfer file FTP jika kapasitasnya sudah penuh. Selain itu, dengan membatasi kapasitas FTP, hacker menjadi tak tertarik untuk upload file-file sampah di server FTP.
- Pembatasan waktu login: Beberapa sistem operasi juga memungkinkan pembatasan waktu login. Ini akan membatasi akses FTP, sehingga user dapat menyetor file pada waktu-waktu yang diizinkan saja.
- Pembatasan IP: Umumnya, sistem operasi modern dapat melakukan pembatasan akses FTP dari IP tertentu. Ini akan secara signifikan mengurangi ancaman ke server Anda.
- Gunakan password yang kuat bagi user: Password yang baik dan kuat akan melindungi user dari hacker-hacker yang ingin mencuri account. Beberapa sistem operasi ada fitur untuk mengaktifkan Password harus memenuhi persyaratan secara langsung atau '*Passwords Must Meet Complexity Requirements*'. Ciri password yang baik adalah: Tidak menggunakan nama user, minimal 6 karakter, sebisa mungkin menggunakan kombinasi dari 4 kategori, yaitu huruf besar, huruf kecil, angka, dan karakter non angka (misalnya !, \$, #, %).

## **3.2 Hypertext Transport Protocol (HTTP)**

Hypertext Transport Protocol atau http digunakan untuk mengakses halaman teks yang disusun menggunakan format khusus yang disebut *Hypertext Markup Language* atau HTML. Tag HTML dimasukkan ke dokumen web untuk memformat jenis font, warna, posisi teks, dan atribut tampilan halaman web lainnya.

Yang penting dari HTML adalah kemampuannya untuk membuat link, sehingga satu halaman bisa me-link ke halaman yang lain, file, dan website lain. Sehingga, pengunjung bisa berpindah ke tempat lain dengan mudah dengan mengklik link dari satu halaman.

### **3.2.1 Metode Pemformatan HTML**

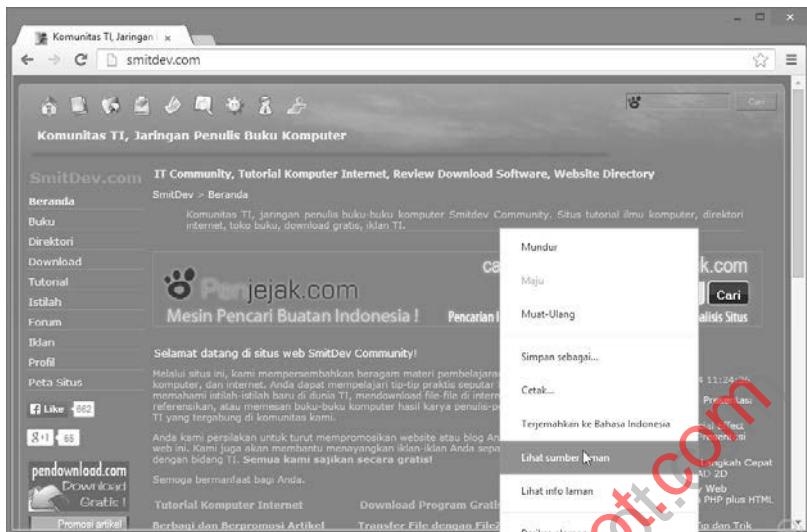
Protokol HTTP merupakan protokol dengan sedikit kode. Kode yang penting adalah GET untuk mendapatkan file HTML ukuran kecil. HTML sendiri merupakan sebuah blok teks yang dilingkupi oleh tag-tag tertentu.

Tag pembuka akan menginstruksikan browser untuk melakukan sesuatu hal, misalnya <TITLE> untuk memulai menampilkan judul halaman. Sementara, tag penutup seperti </TITLE> akan memerintahkan browser untuk berhenti melakukan sesuatu yang dibuka sebelumnya. Tag HTML sendiri memiliki banyak variasi yang memungkinkan seorang programmer ataupun desainer web membuat efek halaman web yang modern.

Misalnya, ada command <img src="" /> yang berfungsi untuk memasukkan gambar di halaman web. Dengan demikian, halaman HTML akan bisa berisi gambar-gambar di dalamnya.

Hyperlink juga cukup penting, karena memungkinkan user untuk mengklik link tersebut yang akan membawanya ke halaman web lain. Membuat halaman tersebut interaktif, mudah diatur, dan cepat diakess.

Untuk melihat kode HTML, Anda tinggal klik kanan pada sembarang tempat di browser, kemudian mengklik menu **View Source** atau **View Page Source** tergantung browser yang Anda pakai. Jika ada bahasa Indonesia di browser, mungkin menu tersebut diterjemahkan sebagai **Lihat Sumber Halaman**.



Gambar 3.4 Menu untuk melihat kode sumber halaman

```
<!DOCTYPE html>
<html lang="id">
<html xmlns:fb="http://ogp.me/ns/fb#>
<head>
<meta http-equiv="Content-Type" content="text/html; charset=UTF-8"/>
<title>Komunitas TI, Jaringan Penulis Buku Komputer - SmitDev</title>
<meta name="description" content="Komunitas TI, Jaringan penulis buku-buku komputer Smitdev Community. Situs tutorial ilmu komputer, direktori internet, toko buku, download gratis, iklan TI."/>
<meta name="keywords" content="smitdev, komunitas, generbit, teknologi, web, website, situs, direktori, download, program, jaringan, penulis, buku komputer, istilah, iklan, internet, software, tutorial, artikel"/>
<meta name="language" content="id"/>
<meta name="robots" content="index,follow"/>
<meta content="2a38213919d4d615fa5c6ef3d30f9" name="verifikasi-penjejak"/>
<meta name="author" content="SmitDev Community" />
<meta name="copyright" content="SmitDev Community" />
<meta name="creator" content="SmitDev Community" />
<meta name="revisit-after" content="72 days" />
<meta http-equiv="image/png" content="false" />
<meta property="og:title" content="SmitDev Community" />
<meta property="og:type" content="company" />
<meta property="og:url" content="http://www.smitdev.com/" />
<meta property="og:site_name" content="SmitDev Community" />
<meta property="og:image" content="555131648" />
<link href="http://www.smitdev.com/templates/smitdev_community/screen.css" rel="stylesheet" type="text/css"/>
media="screen" />
<link href="http://www.smitdev.com/templates/smitdev_community/print.css" rel="stylesheet" type="text/css"/>
media="print" />
<link rel="shortcut icon" href="http://www.smitdev.com/favicon.ico" type="image/x-icon" />
<link rel="alternate" type="application/rss+xml" title="RSS 2.0" href="http://www.smitdev.com/feed/rss.xml" />
<link rel="alternate" type="application/rss+xml" title="ROR" href="http://www.smitdev.com/ror.xml" />
<script type="text/JavaScript">
</i-->
Menunggu smitdev.com... 1.0
```

Gambar 3.5 Kode sumber halaman

Tidak hanya menampilkan teks, gambar, dan foto, kini muncul banyak layanan web yang membuat protokol HTTP ini menjadi layanan internet yang paling banyak diakses. Salah satu yang terkenal adalah layanan iklan via web.

Dengan adanya iklan, web mulai menjadi media komersil dan mulai bersifat strategis. Untuk itu, dikembangkanlah scripting untuk keperluan ini, baik bahasa scripting berbasis klien atau bahasa scripting berbasis server.

Script di halaman web merupakan sebuah kode yang meng-eksekusi perintah tertentu. Menggunakan script, browser dapat mengeksekusi fungsi tertentu sesuai dengan kode script tersebut. Aksi yang dapat dilakukan dapat bervariasi, mulai dari sederhana hingga kompleks.

Nah, script ini juga bisa disalahgunakan untuk melakukan sesuatu yang jahat. Misalnya, seorang programmer bisa membuat halaman web menampilkan sesuatu yang seharusnya tidak diperbolehkan, baik sumbernya di server atau di client.

Hasilnya bisa sekedar tampilan yang berubah atau hingga sistem server atau client crash. Misalnya, script yang melakukan loop hingga tak terhingga jika diterapkan di server bisa membuat server hang, sementara jika diterapkan di client bisa menyebabkan browser hang atau bahkan komputer client menjadi hang.

Karena itu, para pengatur standarisasi web sudah bekerja keras untuk menghasilkan spesifikasi yang memungkinkan scripting dilakukan dengan aman. Namun, tentu saja teknologi tetap memiliki kekurangan, karena itu selalu saja ditemukan lubang celah keamanan baru yang memungkinkan orang jahat untuk melakukan hal yang tidak diperbolehkan.

Sebagai pencegahan, browser-browser modern umumnya menyediakan fitur untuk men-disable script atau applet. Atau menjalankannya dalam mode terbatas.

### 3.2.2 Apa itu Script?

Istilah script sudah digunakan cukup lama, yaitu sejak tahun 1970an. Istilah ini awalnya kerap digunakan di lingkungan sistem operasi Unix. Ketika itu, istilah script mengacu pada perintah shell script yang merupakan perintah yang dibaca oleh komputer dari sebuah file. Dengan menggunakan script di Unix tersebut, banyak perintah dapat diakses sekaligus. Karena itulah script sebenarnya hanya istilah yang menyatakan kode yang bisa diakses.

Nah, script sekarang dapat juga dikaitkan ke halaman web. Ini disebabkan bahasa scripting sudah meningkat fleksibilitas dan kehandalannya. Khusus untuk dunia web, script bisa diakses di server ataupun di client.

Keuntungan scripting berbasis client adalah eksekusi di client, sehingga aksesnya cepat. Ini memberikan efek instan di halaman web. Ini misalnya cocok digunakan untuk mengecek pengisian textbox-textbox di form yang harus diinput oleh user. Sehingga, admin web dapat menghindari adanya kesalahan saat data masih di client dan belum masuk ke database server yang nantinya lebih sulit untuk diperbaiki.

Namun, scripting di client juga ada kelemahannya, yaitu kode dan data bisa terlihat oleh user mengingat kode client side ini bisa dilihat karena berupa plain text.

Karena itu, ada keuntungannya menggunakan scripting berbasis server, yaitu bisa lebih mengakomodasi kerahasiaan. Proses yang dipanggil atau kodennya berada di komputer server, sehingga tidak mudah dianalisis atau diintip.

Selain itu, bisa juga proses yang diproses di server tersebut lebih memakan resource, sehingga sulit untuk dijalankan di komputer client. Atau bahkan akan membuat komputer klien hang jika dipaksakan. Sebabnya, karena pada umumnya komputer server lebih memiliki kapasitas hardware dibandingkan dengan komputer client. Apa pun proses yang terlalu kompleks, ataupun mengakses database, lebih baik dijalankan secara server-side.

Saat ini dan di masa depan, dunia web senantiasa sedang berbenah. Script pun mulai distandarisasi dan teknik untuk menjalankan script pun diperbaiki agar lebih baik lagi. Saat ini, baik script ataupun kode HTML sudah distandarisasi menggunakan paradigma XML dalam bentuk XHTML. Koneskuensinya, nantinya mempermudah browser di berbagai platform untuk mengakses halaman web.

Ada juga AJAX yang memungkinkan user untuk berinteraksi dengan script di server menggunakan script client side, sehingga efeknya adalah seketika, seolah aplikasi desktop yang tak perlu melakukan refresh untuk melihat perubahan aksi.

### **3.2.3 Scripting Berbasis Client**

Ada 2 jenis scripting, yaitu yang berbasis client dan yang berbasis server. Dari kedua jenis itu, yang paling sering dipakai adalah yang berbasis client atau sering disebut client-side.

Scripting berbasis client pun beragam, ada yang bisa diakmodasi oleh banyak browser karena sifatnya yang terbuka dan terstandarisasi, namun ada juga yang sifatnya tertutup, sehingga hanya cocok untuk beberapa browser saja.

Kadang, browser perlu untuk menambahkan sebuah program tertentu untuk bisa menampilkan script berbasis client tersebut. Program tambahan tersebut disebut plug-in yang merupakan program tambahan untuk browser tersebut.

Misalnya, applet Java yang memerlukan plugin JRE untuk sistem operasi dan browser, sehingga kode client side untuk mengakses file flash di server dapat berjalan.

Berikut ini beberapa bahasa pemrograman client side yang populer:

- JavaScript
- VBScript
- Java (memerlukan plugin)
- Kontrol ActiveX
- Macromedia Flash (memerlukan plugin)

Seorang bisa membuat lebih dari satu script dalam waktu yang bersamaan. Namun, bahasa tidak bisa dicampur dalam satu potong script. Dari 5 script populer di atas, yang paling populer adalah JavaScript.

Ini disebabkan karena JavaScript (berbeda dengan Java) yang merupakan bahasa scripting yang pertama kali muncul dan sifatnya terbuka, sehingga didukung oleh banyak browser dan paling banyak diimplementasikan.

JavaScript pertama kali diperkenalkan oleh Netscape Navigator yang kemudian diadopsi oleh Microsoft dengan nama JScript. Ditinjau dari tata bahasanya, JavaScript dikembangkan berbasis C, C++, dan Perl.

Sementara VBScript adalah script yang dikembangkan oleh Microsoft yang berbasis bahasa Visual Basic. Sintaks VBScript sejauh ini hanya bisa dieksekusi oleh browser yang dikembangkan oleh Microsoft pula, yaitu Internet Explorer. Untuk browser lain juga bisa, namun perlu plugin.

Yang ketiga adalah Java (berbeda dengan JavaScript). Untuk menggunakan Java, diperlukan plugin. Walaupun demikian, Java juga termasuk plugin yang populer karena bisa diakses di banyak browser dan di berbagai platform asalkan memiliki plugin Java Runtime environment atau lazim disingkat sebagai JRE.

Untuk menjalankan script Java, programmer harus menuliskan kode Java kemudian mengkompilasinya. Setelah terkompilasi, program akan bisa dijalankan di semua komputer atau piranti yang memiliki JRE.

Script Java yang berbasis client sering juga disebut sebagai applet. Adapun yang dijalankan di server sering juga disebut servlet. Berbeda dengan lainnya, Java merupakan script yang cukup powerful karena adanya environment khusus yang memungkinkan kode Java untuk dijalankan. Walaupun demikian, JRE memiliki security manager yang memungkinkan kode Java untuk tidak mengakses bagian penting dari sistem operasi yang bisa membuat komputer tidak stabil atau hang. Namun, script Java juga bisa digunakan untuk melakukan hal yang jahat. Kode jahat ini sering disebut juga sebagai malicious applet atau applet jahat.

Adapun ActiveX merupakan bahasa pemrograman yang memiliki berbagai kemampuan sekaligus berpotensi mengundang bahaya. Kontrol-kontrol ActiveX bisa diintegrasikan ke halaman web dan menggunakan berbagai fungsi seperti button, list drop down, textbox, dan sebagainya.

Karena bersifat strategis, kontrol ActiveX bisa mengambil alih mesin host yang dipakai untuk menjalankan halaman web. Akibatnya, jika ada kode jahat, ActiveX bisa menjadi worm yang akan menyebabkan kerusakan komputer.

Tidak seperti Java yang ada security manager-nya, ActiveX sangat powerful, sehingga sangat mungkin disalahgunakan. Tapi, ActiveX merupakan sebuah tool yang powerful dan fleksibel, sehingga sangat menarik bagi programmer dan pengembang web.

### **3.2.4 Scripting Berbasis Server**

Ketika script berbasis server dieksekusi, maka proses pengeksekuksian script dilakukan di server, dan user hanya melihat hasil akhirnya (jika script mengeluarkan pemberitahuan ke client). Jika tidak ada, maka user tidak akan melihat apa-apa ketika script tersebut melakukan proses tertentu.

Contoh penerapan scripting berbasis server, misalnya ketika halaman web hendak menyetor data ke database di server, melalui form atau melalui lainnya.

Salah satu ciri bahasa server side adalah ada komunikasi di server, atau dengan kata lain ada konsumsi bandwidth ke server. Untuk berkomunikasi, ada 2 jalur yang lazim dipakai, pertama adalah komunikasi secara langsung, yang kedua menggunakan Common Gateway Interface (CGI).

Common Gateway Interface (CGI) merupakan sebuah lapisan perantara antara server dan client. CGI lah yang menentukan aturan di mana berbagai program saling berkomunikasi. Tujuan CGI adalah menerjemahkan antara berbagai bahasa dan sistem yang berbeda. Program CGI bisa ditulis di berbagai bahasa seperti C, C++, Java, Perl, dan Visual Basic.

Beberapa bahasa pemrograman berbasis server yang populer antara lain:

- PHP
- Perl
- Active Server Pages (ASP)
- ColdFusion
- Java Server Pages (JSP)
- Python
- Ruby

Karena berbasis server, pemilihan bahasa yang digunakan akan tergantung software server yang diinstal di komputer server. PHP memerlukan software PHP parser, begitu pula lainnya. Dari segi penulisan, Perl, PHP, dan Ruby bahasanya mirip dengan C, C++, atau Java.

Penting juga pertimbangan masalah sistem operasi untuk menjalankan server. Bahasa script open source biasanya dapat diakomodasi oleh berbagai platform sistem operasi, namun yang komersil seperti ASP hanya bisa diakses dari sistem operasi Windows.

Pemilihan bahasa pemrograman akan memengaruhi bagaimana halaman web yang dihasilkan. Namun, pemilihan bahasa pemrograman juga bisa menjadi sumber masalah. Sebabnya karena tiap bahasa pemrograman memiliki kelemahan dan bug sendiri yang bisa dieksloitasi oleh penyerang. Sehingga, programmer harus waspada dengan bahasa pemrograman yang dipilihnya.

### 3.2.5 Serangan di Web dan Pencegahannya

Karena sifat scripting ada 2 jenis, client dan server, maka serangan di web pun ada 2 jenis, client dan server. Tiap jenis serangan web tersebut memiliki variasinya sendiri-sendiri.

Untuk serangan web yang bersifat client-side, contohnya seperti berikut:

- Tag HTML yang berpotensi jahat: Kode jahat yang disisipkan di halaman atau bisa juga disebabkan oleh penulisan kode yang salah secara logika ataupun penulisan syntax-nya, bisa menyebabkan server menampilkan halaman yang berbahaya jika dijalankan di server, sehingga membuat server hang. Ini misalnya di pembuatan form.

Pencegahannya adalah programmer web atau orang yang membuat halaman web harus benar-benar membuat form yang tervalidasi dan tidak akan memproses form yang belum tervalidasi. Karena itu, validasi client side umumnya yang dipakai di sini.

- Kode jahat di client: Bisa jadi seorang yang memiliki akses ke server bisa menambahkan script client-side yang jahat ke halaman dokumen. Misalnya yang mengandung loop yang tak terhingga, pembagian dengan nol (*divided by zero*), dan berbagai algoritma lain yang memungkinkan browser hang, dan akhirnya komputer bisa jadi hang.

Sebagai pencegahan, Anda dapat mematikan fasilitas script di komputer. Misalnya untuk Firefox, Anda dapat mengetikkan **about:config**. Kemudian, ketikkan kata kunci “java” untuk menyaring kata kunci berkaitan dengan java.

Nama Pengaturan	Status	Jenis	Nilai
browser.urlbar.filter.javascript	default	boolean	true
dom.ipc.plugins.java.enabled	default	boolean	false
javascript.enabled	default	boolean	true
javascript.options.asmjs	default	boolean	true
javascript.options.baselinejit.chrome	default	boolean	true
javascript.options.baselinejit.content	default	boolean	true
javascript.options.gc_on_memory_pressure	default	boolean	true
javascript.options.ion.chrome	default	boolean	false
javascript.options.ion.content	default	boolean	true
javascript.options.ion.parallel_compilation	default	boolean	true
javascript.options.jit_hardening	default	boolean	true
javascript.options.mem_gc_allocation_threshold_mb	default	bilangan bulat	30
javascript.options.mem_gc_decommit_threshold_mb	default	bilangan bulat	32
javascript.options.mem_gc_dynamic_heap_growth	default	boolean	true
javascript.options.mem_gc_dynamic_mark_slice	default	boolean	true
javascript.options.mem_gc_high_frequency_heap_growth_max	default	bilangan bulat	300
javascript.options.mem_gc_high_frequency_heap_growth_min	default	bilangan bulat	150
javascript.options.mem_gc_high_frequency_high_limit_mb	default	bilangan bulat	500
javascript.options.mem_gc_low_frequency_low_limit_mb	default	bilangan bulat	100
javascript.options.mem_gc_low_frequency_time_limit_ms	default	bilangan bulat	1000
javascript.options.mem_gc_incremental	default	boolean	true
javascript.options.mem_gc_incremental_slice_ms	default	bilangan bulat	10
javascript.options.mem_gc_low_frequency_heap_growth	default	bilangan bulat	150
javascript.options.mem_gc_per_compartment	default	boolean	true
javascript.options.mem.high_water_mark	default	bilangan bulat	128

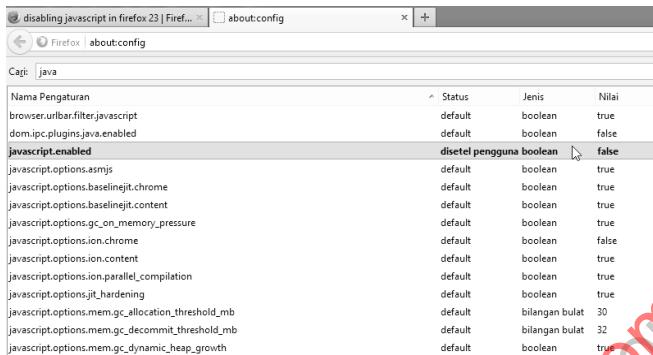
Gambar 3.6 About:config

Klik dua kali pada **javascript:enabled** untuk menonaktifkan javascript.

Nama Pengaturan	Status	Jenis	Nilai
browser.urlbar.filter.javascript	default	boolean	true
dom.ipc.plugins.java.enabled	default	boolean	false
<b>javascript.enabled</b>	default	boolean	true
javascript.options.asmjs	default	boolean	true
javascript.options.baselinejit.chrome	default	boolean	true
javascript.options.baselinejit.content	default	boolean	true
javascript.options.gc_on_memory_pressure	default	boolean	true
javascript.options.ion.chrome	default	boolean	false
javascript.options.ion.content	default	boolean	true
javascript.options.ion.parallel_compilation	default	boolean	true
javascript.options.jit_hardening	default	boolean	true
javascript.options.mem_gc_allocation_threshold_mb	default	bilangan bulat	30
javascript.options.mem_gc_decommit_threshold_mb	default	bilangan bulat	32
javascript.options.mem_gc_dynamic_heap_growth	default	boolean	true
javascript.options.mem_gc_dynamic_mark_slice	default	boolean	true

Gambar 3.7 Klik 2x untuk menonaktifkan javascript

Kalau sudah bernilai false, artinya javascript sudah tidak dapat dijalankan di Firefox.



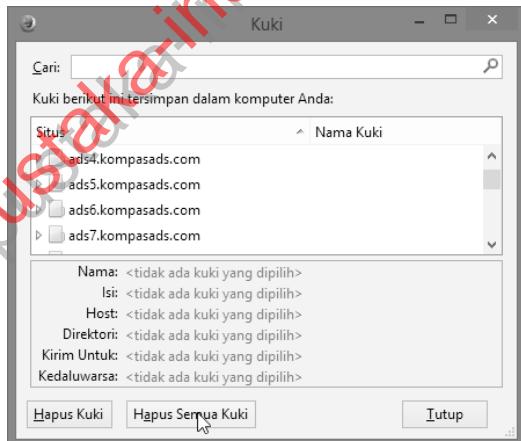
Gambar 3.8 Set `javascript:enabled` ke False

- Penyalahgunaan tag: Tag seperti `<form>` pada umumnya tidak berbahaya, namun bisa juga menjadi bahaya jika di embed di tempat yang salah. Karena nantinya penyusup bisa mengintip informasi sensitif dengan memodifikasi perilaku form atau yang sudah diinput oleh user yang sebelumnya mengisikan data di form. Tag HTML lain juga bisa berpotensi mengubah tampilan halaman, memasukkan atau mengganti gambar, sehingga website menjadi berubah bentuk dan tampilannya. Sebagai perubahan, Anda dapat mengeset security browser ke **High**.
- Penyalahgunaan cookies: Ketika seorang mengunjungi website, sebuah file plain text sederhana otomatis dibuat dan diletakkan di browser yang nantinya dapat diakses oleh browser. Di kunjungan selanjutnya, server akan menindai apakah ada cookies yang sudah ada di komputer. Di cookies, tersimpan beberapa informasi yang memungkinkan server mengenali orang atau aktivitas yang dilakukan sebelumnya. Nah, cookies ini bisa disalahgunakan, sehingga orang yang tidak berhak untuk mengakses email atau account lain (seperti Facebook atau Instagram) bisa login dengan mudah. Cookies juga bisa memicu download secara tidak diinginkan. Cara menghapusnya dengan klik tab **Privasi** di pengaturan, kemudian klik **Menghapus kuki satu per satu**.



Gambar 3.9 Setting untuk menghapus cookies

Setelah itu, klik pada tombol **Hapus semua kuki** untuk menghapus semua kuki, atau klik pada tombol **Hapus kuki** untuk menghapus kuki terpilih saja.



Gambar 3.10 Menghapus cookies

- Browser kadaluarsa: Browser yang kadaluarsa rentan terhadap kesalahan pengeksekusian script, sehingga bisa hang dan akhirnya membuat komputer hang. Untuk itu, Anda perlu menghindari browser kuno, terutama Internet Explorer (IE) 6. Gunakan IE versi terbaru jika Anda menginginkan untuk menggunakan IE.

Jenis serangan web yang kedua adalah serangan di sisi server. Ada beberapa yang sering Anda temui, antara lain:

- Buffer overflow: Ini merupakan jenis serangan ke server yang cukup berat. Di sistem operasi, ketika ada kebutuhan memory yang besar secara mendadak, maka sistem operasi ada error, karena pengaturan memory menjadi kacau. Hasilnya komputer bisa berlaku tak wajar dan crash.

Salah satu teknik serangan buffer overflow adalah menggunakan kode backdoor. Teknik lainnya adalah menginstal software yang memungkinkan account penyerang ditingkatkan menjadi administrator.

Sebagai pencegahan untuk buffer overflow adalah web diprogram dengan lebih baik, sehingga tidak ada input user yang bisa disalahgunakan hingga membuat server bekerja keras. Misalnya, divide by zero atau loop tak terbatas.

- Salah guna cookies: salah guna cookies juga bisa berpengaruh di server. Terutama jika server meng-host aplikasi yang berkaitan dengan uang, seperti menghost nomor kartu kredit, e-commerce, dan sebagainya. Ada juga XSS (*Cross Site Scripting*) yang memungkinkan user untuk mengeksekusi perintah di server dengan memasukkan URL atau script di client.

Sebagai pencegahan, adalah memprogram web agar tidak mudah punya kelemahan XSS. Selain itu juga dengan tidak terlalu menggantungkan pada cookies, perlu penyimpanan informasi di client menggunakan metode lain.

- ActiveX yang disalahgunakan: Di platform .NET, ActiveX memungkinkan interaksi seperti Java, namun lebih powerful. Karena itu ActiveX yang mengandung kode yang jahat bisa mengakses sistem operasi. Karena itu, Anda bisa men-disable akses ActiveX di browser.

### **3.3 Domain Name Service (DNS)**

Domain Name Service berguna untuk mempermudah mencari nama URL ke pengguna internet. Anda pasti akan lebih mudah mengenal WWW.nama\_domain.com dibandingkan 124.5.124.32. Server yang menerjemahkan IP address ke angka dan sebaliknya disebut DNS server.

Seperti halnya protokol lainnya di internet, DNS memiliki kelemahan sendiri. DNS digunakan untuk mencari nama yang user friendly dari IP dan sebaliknya.

DNS diperlukan karena internet dijalankan dengan IP address, adapun manusia lebih mudah mengingat kata dibandingkan IP address. Nah, layanan DNS ini menyediakan direktori yang terdistribusi yang memungkinkan user untuk mengetik URL dan kemudian DNS akan mencari IP address dari alamat yang diketikkan tersebut.

DNS umumnya tidak merupakan prioritas pertama ketika mencari IP address. Yang pertama dicari adalah tabel alamat yang sudah disimpan di cache komputer agar tidak memboroskan bandwidth. Baru ketika komputer tidak menemukan yang dicarinya, maka komputer akan menghubungi DNS server terdekat apakah DNS server tersebut memiliki daftar IP address atau tidak? Jika DNS server juga belum menemukan, maka DNS server akan menghubungi DNS yang terdekat hingga akhirnya mendapatkan alamat yang diinginkan. Jika ternyata belum ada, maka akan terlihat tampilan error di browser.

Karena itu, serangan bisa dilakukan dengan 3 variasi:

- Pertama adalah mengubah cache di komputer lokal dengan data yang salah. Sehingga, jika user mencari cache, maka akan dialamatkan ke alamat yang salah.
- Yang kedua adalah Anda mengubah atau menambah data yang salah di DNS server. Jika DNS server tersebut merupakan DNS utama di sebuah ISP atau negara tertentu, maka Anda akan menyesatkan banyak pengunjung internet. Namun, karena arsitektur DNS yang berjaringan, maka ini efeknya tak akan lama, karena ada backup DNS yang siap mengembalikan kondisi.

- Yang ketiga adalah menghalangi akses ke DNS server dari jaringan tertentu atau ISP terkenal yang digunakan. Salah satu metode untuk melakukan ini, pertama menyerang server DNS, sehingga layanan DNS server hang atau rusak. Jika DNS rusak, maka komputer juga tidak bisa mengakses layanan seperti email, FTP, dan sebagainya, karena semuanya menggunakan DNS untuk mencari tahu hostname.

Karena DNS umumnya diakomodasi oleh pihak luar, maka Anda tidak bisa melakukan pencegahan. Anda hanya bisa berharap semoga admin DNS selalu meng-update DNS servernya dan merecover secepatnya jika ada serangan.

### **3.4 Dynamic Host Configuration Protocol (DHCP)**

Ketika diminta, DHCP otomatis mengalokasikan alamat Internet Protocol atau IP address, seperti 172.16.32.15 ke komputer di jaringan lokal. Sebuah IP address diperlukan untuk berkomunikasi dengan piranti lain di jaringan, sehingga antar komputer bisa saling mentransfer data.

Untuk bisa mengakses internet, user perlu alokasi IP address. Namun, bisa jadi IP address yang ada terbatas atau terlalu repot jika mengalokasikan IP address satu demi satu, padahal jumlah komputer ratusan buah. Untuk itu, Anda dapat menggunakan DHCP yang akan mengalokasikan IP address secara otomatis.

DHCP menyediakan IP address ke user yang sudah login. Jadi ketika user baru login, user tersebut akan memperoleh IP address. Ketika user logout, maka IP address tersebut bisa diberikan ke user lain yang baru login.

Selain DHCP, ada juga istilah NAT (*Network Address Translation*) yang merupakan teknik populer untuk membagi IP address yang sama ke lebih dari satu user. Tapi, alamat ini tidak akan tampak ke dunia luar. Jaringan NAT biasanya menggunakan alokasi private address.

Serangan ke DHCP server umumnya melibatkan interupsi pada proses pembagian IP address. Serangan ke DHCP bisa juga diarahkan ke DNS server karena jika DNS error, maka DHCP juga error dan menghasilkan informasi yang salah, sehingga komputer tidak akan mampu untuk terhubung ke internet.

Teknik lainnya yang populer adalah mengubah assignment pool, sehingga DHCP mulai mengeluarkan IP address yang invalid. Untuk mencegahnya, admin DHCP harus selalu memastikan software DHCP server-nya selalu uptodate.

Ada juga teknik yang disebut DHCP starvation yang merupakan serangan dengan cara menyebarkan request DHCP dengan Mac Address yang diubah. Tool untuk melakukan ini misalnya software Goobler.

Jika permintaan IP address terlalu banyak, maka penyerang dapat menghabiskan space IP address di DHCP server selama beberapa waktu tertentu. Sehingga, user yang asli malah tidak bisa mendapatkan alokasi IP address.

Ini mirip serangan DOS (*denial of service*) yang akan menyibukkan server DNS. Cara penanganannya adalah dengan membatasi jumlah Mac Address di port yang ada di Switch. Namun, serangan ini juga makin sulit dilakukan karena dibuatnya standardisasi baru untuk DHCP.

### 3.5 Konten Tak Layak

Ancaman online yang lain adalah maraknya konten tak layak di web. Ini sebenarnya bagian dari HTTP, tapi karena ruang lingkupnya yang berbeda, maka dibahas tersendiri.

Internet (WWW) merupakan hutan rimba belantara, *gung liwang liwung*, yang tidak memiliki aturan. Semua konten bisa diakses, termasuk konten tak layak yang bisa diakses oleh sembarang orang.

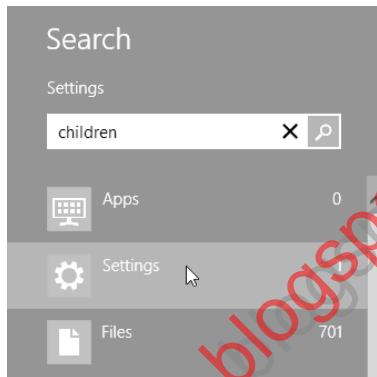
Untuk itu, Anda dapat memproteksi menggunakan beberapa software, baik software yang ada di browser atau sistem operasi. Software untuk melakukan ini disebut software web filter.

### 3.5.1 Family Safety

Untuk meminimalkan efek dari konten tak layak, Windows 7 dan 8 mulai memiliki fitur Family Safety. Ini bisa membatasi user tertentu (misalnya anak-anak) dalam mengakses layanan Windows, termasuk browsing.

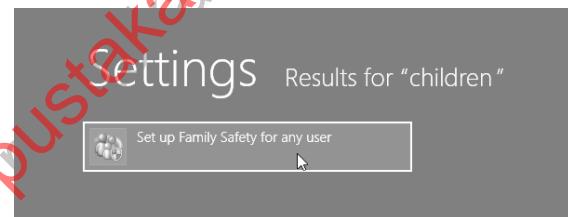
Cara menggunakan family safety ini adalah:

1. Tekan **Windows + F** hingga muncul jendela **Search**. Isikan "children".



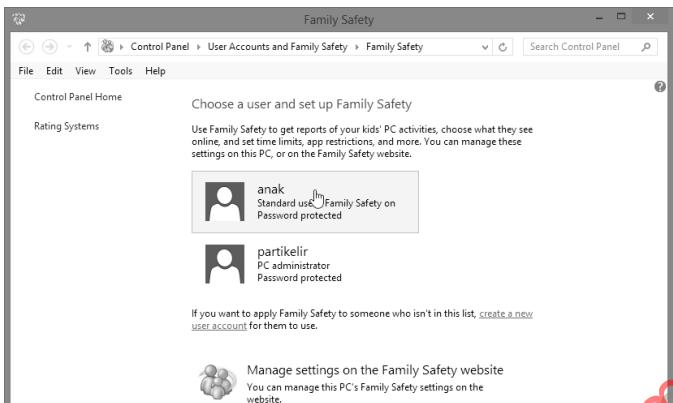
Gambar 3.11 Muncul jendela Search

2. Klik **Settings**, kemudian klik hasil pencarian **Set up family safety for any user**.



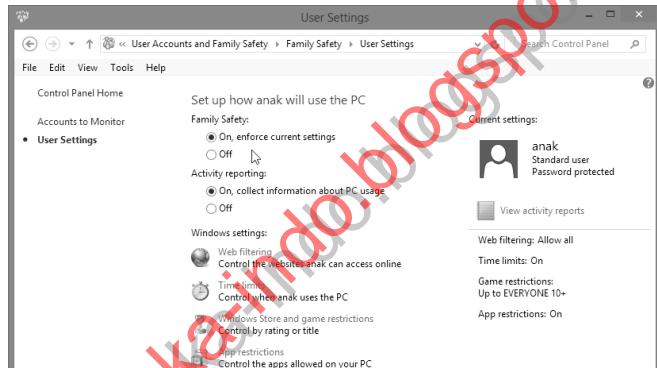
Gambar 3.12 Klik Set up family safety for any user

3. Kemudian, pilih user yang akan diatur family safety-nya, admin tidak bisa diberi family safety. Karena itu, kalau belum memiliki user yang akan dialokasikan, buat user baru baru, kemudian klik di **Choose a user and setup family safety**.



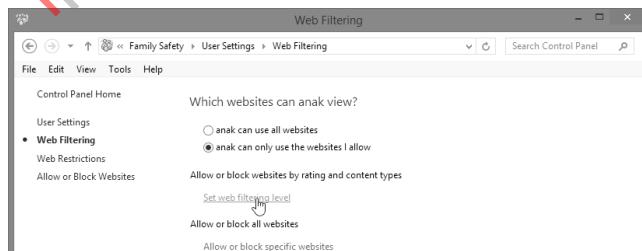
Gambar 3.13 Klik Choose a user and setup family safety

#### 4. Untuk mengaktifkan, klik On di Family safety.



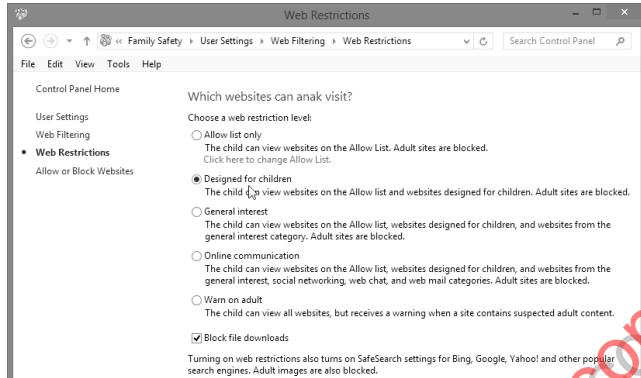
Gambar 3.14 Mengaktifkan family safety di User settings

#### 5. Untuk memfilter web yang bisa dilihat, klik pada Web Filtering.



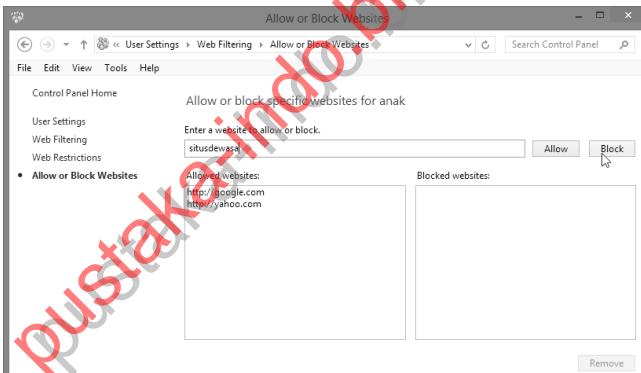
Gambar 3.15 Klik pada Web filtering

6. Pilih kategori website yang ingin dialokasikan, misalnya **Designed for Children**.



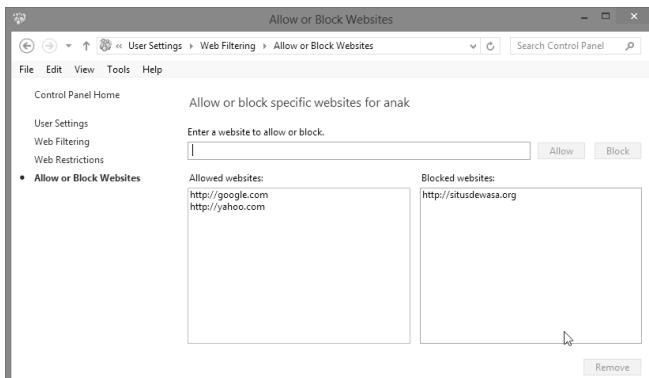
**Gambar 3.16 Menentukan kategori website yang boleh dibuka**

7. Di **Allow or block website**, Anda bisa memasukkan situs-situs yang ingin diblok atau dibolehkan. Masukkan pada kotak teks, kemudian klik **Allow** untuk mengizinkan atau **Block** untuk memblok.



**Gambar 3.17 Allow atau block**

8. Daftar situs yang dibolehkan dan diblok akan ditampilkan di **Allowed websites** dan **Blocked websites**.

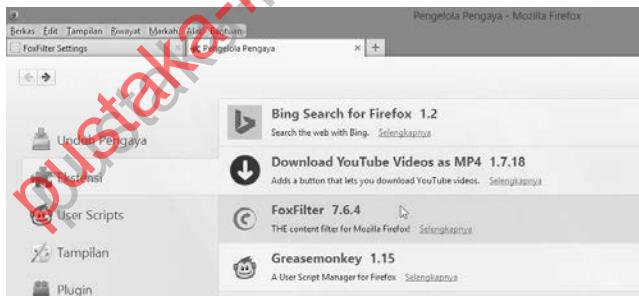


Gambar 3.18 Daftar Allowed websites dan blocked websites

### 3.5.2 FoxFilter

Sementara untuk browser Firefox, ada banyak plugin untuk keperluan web filtering ini. Satu yang bagus adalah FoxFilter. Cara menginstal foxfilter adalah:

1. Buka Firefox Anda, kemudian buka halaman Extensions/ Pengaya dengan mengklik Ekstensi > Pengaya atau dalam bahasa Inggris adalah Extension > Add-ons. Kemudian, cari FoxFilter dan install, saat sudah terinstal, terlihat Fox-Filter ada di halaman Pengelola Pengaya seperti berikut.



Gambar 3.19 Klik Extension > Add ons

2. Klik halaman **Settings**, maka muncul halaman setting. Di **Filtering preferences**, Anda bisa atur pengaturan filtering.

The screenshot shows the 'FILTERING' tab selected in the top navigation bar. Below it, the 'Filtering Preferences' section is displayed. It contains three radio button options: 'Enable filtering based upon Blocked websites, keywords and Sensitivity Settings' (selected), 'Only allow access to Trusted sites that I have specified', and 'Turn off FoxFilter (see the auto-enable feature below)'. A note below asks if users want to auto-enable FoxFilter when Firefox starts, with three checkboxes: 'Yes, auto-enable FoxFilter when Firefox is started, using my filtering preference below' (checked), 'Auto-enable filtering based upon blocked websites, keywords and sensitivity settings', and 'Auto-enable access only to my Trusted sites'.

**Gambar 3.20 Pengaturan Filtering preferences**

3. Di **Blocked Websites and Keywords**, masukkan daftar kata kunci yang apabila dideteksi oleh FoxFilter akan langsung diblok situsnya.

#### Blocked Websites and Keywords

Enter keywords (e.g. 'porn') and website names (e.g. 'playboy.com') below. You can insert new entries anywhere in the list or use cut & paste. When saved, the list will be automatically sorted for you.

Website Example: Entering a domain name such as 'playboy.com', 'penthouse.com', etc. will instruct FoxFilter to block ALL pages on the site.

Keyword Example: Entering specific keywords such as sex, porn, etc. will instruct FoxFilter to block any page that contains the specific keyword. Entering a keyword with 'and', such as 'free and sex' will make sure that both keywords are detected before blocking the content.

Please use our FAQ link on this page for more information.



**Gambar 3.21 Pengisian kata kunci untuk memblok website**

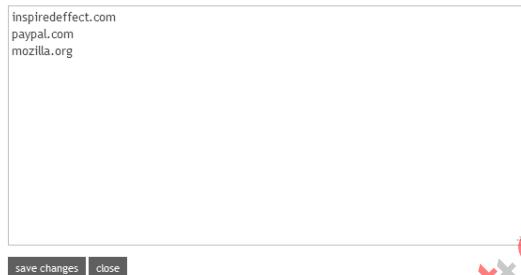
4. Di **Trusted sites**, masukkan situs-situs terpercaya. Situs terpercaya ini akan tetap bisa dilihat walaupun ada kata kunci yang seharusnya diblok.

## Trusted Sites

Add trusted sites, such as Yahoo.com, that may contain a keyword such as 'sex' or 'porn', but that you still consider safe.

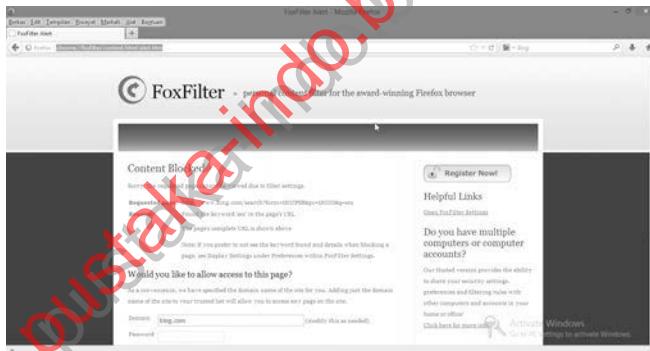
Tips: When adding a trusted site, it is recommended that you enter only the primary domain name (e.g. yahoo.com, google.com, etc.). It is not necessary to include the full address (e.g. http://www.yahoo.com). Also, you may choose to just add specific sub-domains to your trusted list (e.g. images.search.yahoo.com, autos.yahoo.com, answers.yahoo.com).

Please use our FAQ link on this page for more information.



**Gambar 3.22 Pengisian Trusted site**

5. Apabila Anda mengetes membuka webpage yang berisi kata yang diblok, otomatis akan muncul halaman bloking seperti berikut.



**Gambar 3.23 Halaman bloking sudah muncul**

## BAB 4

# Up to Date dengan Patch

Yang namanya teknologi selalu berkembang. Begitu pula dengan komputer yang merupakan hasil buah karya teknologi manusia. Berbagai bahasa pemrograman, sistem operasi, algoritma yang digunakan dalam membuat program selalu berkembang dan menghasilkan produk yang lebih baru, lebih sempurna, dan lebih aman.

Kesalahan merupakan tabiat yang diwarisi oleh manusia dan juga hasil karyanya. Tak terlepas di bidang komputer. Software yang dibuat oleh manusia, seperti sistem operasi dan aplikasi selalu memiliki bug, kelemahan yang bisa dieksplorasi oleh orang-orang yang tak bertanggungjawab.

Untuk itulah selalu diperlukan perbaikan berkesinambungan atau *continuous improvement* yang memungkinkan seorang untuk selalu memutakhirkan kondisi software-nya, sehingga lubang-lubang keamanan yang ada selalu mudah untuk ditutupi.

Seorang admin, sering harus memonitor perkembangan software yang digunakannya dan mengetahui masalah-masalah yang muncul di komputernya beserta pemecahan dari permasalahan tersebut. Persoalan selalu ada, dan karenanya proses pemutakhiran software juga adalah sesuatu proses yang berjalan terus-menerus.

## 4.1 Apa Itu Patch?

Patch secara bahasa artinya tambalan. Yaitu, sebuah software berukuran kecil yang dikembangkan sebagai alat untuk menambal lubang-lubang masalah yang ada di software intinya. Jadi, patch bertujuan untuk memperbaiki masalah yang berkaitan dengan sebuah software komputer.

Perbaikan yang dilakukan bisa sekedar menghilangkan bug, mengoreksi kesalahan logika, melengkapi fungsi, dan sebagainya. Walaupun fungsi utamanya untuk menutup kesalahan dan error yang ada, namun patch bisa juga menghasilkan kesalahan atau error baru.

Patch ada berbagai jenis. Untuk software yang komersil (yang source code-nya tertutup), maka patch umumnya diterapkan dalam bentuk biner yang siap dieksekusi dan bukan dalam bentuk source code.

Karena tidak berupa source code, maka patch ini melakukan perbaikan dengan 2 cara. Pertama adalah dengan memodifikasi file biner executable dari program inti, sehingga lubang-lubang error yang ada akan hilang. Sementara yang kedua adalah dengan mengganti file executable inti secara total dengan file executable baru.

Adapun pada software open source yang kode sumbernya terbuka, patch umumnya berupa source code yang merupakan selisih dari source code asli dengan source code perbaikan. Dengan demikian, patch akan mengubah source code dari program yang sudah berjalan dengan program perbaikan. Untuk kasus ini, programmer diwajibkan untuk mengkompilasi source code dari patch, atau bisa juga dengan mengubah file sendiri.

Patch juga bisa diterapkan dalam bentuk rilis software terbaru, yang jika dieksekusi akan memiliki opsi upgrade, remove, atau new installation. Ini diterapkan pada software-software modern.

Jadi, jika ada rilis software yang lebih baru versinya, maka jika software tersebut diinstal, akan otomatis muncul 3 opsi, apakah instalasi software yang lama dihapus, di-update, atau dihapus lalu melakukan instalasi baru. Tipe patch seperti ini lebih praktis, karena instalasi berjalan secara otomatis.

#### **4.1.1 Sumber Patch**

Karena saat ini penetrasi internet sudah rata hampir seluruh dunia, maka sumber mendapatkan patch paling lazim saat ini adalah via internet. Cara mendapatkannya umumnya via download. Dengan demikian, developer atau pengembang software akan dengan mudah meletakkan patch di server web di internet dan kemudian pengguna dapat download patch setiap sekian waktu tertentu.

Patch yang di-download umumnya harus diinstal secara manual karena di-download dalam bentuk file executable. Cara menginstalnya seperti menginstal program baru, yaitu tinggal meng-eksekusi file executable dan kadang perlu menentukan lokasi file executable dari program asli yang di-patch.

Namun, kini program-program yang sering merilis patch merasa lebih praktis jika ada fasilitas auto update. Prinsip sebenarnya masih sama, yaitu patch diletakkan di server dan di-download oleh user, hanya saja proses tersebut diotomasi. Yaitu, adanya sebuah program updater yang otomatis mengecek apakah ada patch baru di internet atau tidak? Jika Ya, maka user dari program akan diberitahu apakah ingin menginstal patch tersebut atau tidak?

Adanya otomatisasi meringankan tugas user karena tidak perlu men-download manual, lalu menginstalnya. Selain itu, umumnya fitur update ini bisa di-tracking, sehingga user mengetahui patch apa saja yang sudah diinstal dan beberapa software updater malah memungkinkan uninstall patch tanpa uninstall program aslinya.

Selain itu, otomatisasi juga membuat proses update berjalan lebih teratur. Contoh program updater yang memungkinkan update otomatis adalah Service pack di Microsoft Windows dan software antivirus yang umumnya sering melakukan update signature virus.

Program updater umumnya meminta persetujuan dari user ketika hendak meng-update, namun ada juga program updater yang langsung meng-upload dan menginstal file patch tanpa pemberitahuan user. Ini berbahaya terutama jika Anda memakai koneksi internet yang tidak bebas kuota alias limited.

Namun, update otomatis juga memudahkan karena membuat Anda tidak perlu menangani satu per satu proses update. Bayangkan, seorang administrator yang punya komputer sampai ratusan/ribuan, maka proses otomatis ini sangat memudahkan pengaturan.

#### **4.1.2 Ukuran Patch**

Ukuran patch bervariasi tergantung ukuran program induknya. Untuk program induk yang berukuran besar seperti sistem operasi, maka patch-nya pun ukurannya bisa puluhan mega bytes. Yang paling kecil bisa hanya beberapa kilobyte.

Ukuran file juga dipengaruhi oleh apa yang hendak dilakukan oleh software patch tersebut. Software patch yang hanya memperbaiki sebagian program akan tidak sebesar ukuran patch yang memperbaiki keseluruhan program.

Ukuran file patch juga besar ketika perubahan ikut pula mengubah file-file yang bukan merupakan bagian file executable atau file inti program, namun file tempat penyimpanan data, seperti database atau file teks untuk menyimpan data. Begitu juga file-file multimedia yang mungkin terlibat, seperti file video atau audio.

Karena itulah patch-patch yang ukurannya besar umumnya patch untuk aplikasi multimedia atau aplikasi yang melibatkan banyak data di database. Namun umumnya, dibandingkan ukuran file installer dari program aslinya, patch masih lebih kecil.

Dari deskripsi di atas, Anda mengetahui bahwa peranan patch penting sekali dalam proses menjaga keamanan dan kehandalan sistem operasi ataupun program aplikasi. Patch lah yang menambal bolong-bolong yang ada di software, sehingga lobang software tertutup yang membuatnya sulit untuk dimasuki kode-kode jahat oleh orang lain.

Kode eksploitasi yang bisa merusak software akan terhalangi berkat patch-patch yang ada. Konsekuensinya? Komputer menjadi lebih aman dan tidak lemah lagi.

Walaupun sebenarnya cukup mudah, tapi ada beberapa orang yang malas mem-patch software-nya. Bisa jadi karena tak adanya koneksi internet, tak ada waktu, atau malas karena patch tak dirasa penting. Ini salah, karena patch adalah teknik pencegahan paling utama. Usahakan untuk mem-patch tiap kali ada patch baru yang dirilis untuk komputer Anda. Untuk sistem operasi Microsoft misalnya, patch dirilis tiap bulan sekali.

## 4.2 Hotfix

Hotfix sebenarnya patch biasa, hanya saja proses patch dilakukan tanpa mensyaratkan software utama harus dimatikan, alias software utamanya masih tetap bisa dijalankan seperti biasa.

Patch-patch modern umumnya mulai mengarah ke jenis hotfix di mana penggunaan komputer oleh user tidak perlu terganggu karena user masih bisa bekerja seperti biasa. Ditinjau dari segi pemasaran, hotfix lebih baik karena memberikan kesan bahwa program lebih handal, selain itu tidak membuat waktu user dalam menggunakan program berkurang.

Sebuah hotfix sama seperti patch biasa, umumnya dipaket dalam bentuk satu paket saja. Hotfix juga bisa digunakan untuk menambahkan fitur di program utama dan bukan sebagai tambahan aspek keamanan.

Masalah yang dihadapi oleh hotfix sama seperti patch, yaitu bisa saja hotfix menutup satu lubang tapi menghasilkan lubang yang lain. Dalam konteks sistem operasi Windows, hotfix adalah sebuah patch kecil yang didesain untuk menangani isu tertentu, misalnya lubang keamanan yang spesifik. Karena itulah, hotfix ukurannya lebih kecil dibandingkan service pack.

Hotfix juga bisa diakomodasi oleh updater otomatis, sehingga user tidak perlu men-download dan menginstal sendiri. Semuanya bisa dilakukan dengan mudah.

Hotfix ini ibarat program, jadi setelah Anda menginstal hotfix, di fitur **Add or Remove programs** Anda akan terlihat bahwa Anda baru saja menginstal hotfix.

## 4.3 Service Pack

Patch dan hotfix merupakan sebuah istilah yang menjelaskan software untuk perbaikan yang berukuran kecil. Namun, sering kali proses perbaikan memerlukan file patch yang ukurannya tidak hanya puluhan mega bytes, namun hingga ratusan mega bytes.

Untuk itulah dihadirkan istilah baru untuk menyebut patch yang berukuran besar di mana patch besar tersebut ditujukan untuk

menghadirkan fitur tambahan atau menutup celah keamanan yang cukup banyak.

Di sistem operasi Microsoft, hal ini disebut service pack. Istilah ini mulai dipakai sejak versi Windows 2000, Windows XP, Vista, Seven, dan rilis Windows berikutnya.

Service pack di Windows disingkat dengan nama SP. Apa saja isinya? Isinya adalah kumpulan patch-patch kecil yang digabungkan dan juga software untuk meningkatkan performa software. Semuanya dapat diinstal hanya dengan sekali instalasi saja.

Jika Anda menyet **Automatic update** menjadi ON, maka setiap kali ada update-an baru akan langsung di-update, tapi itu bukan patch. Karena service pack umumnya harus diinstal terpisah dan bukan lewat automatic update.

Menginstal service pack lebih mudah dibandingkan menginstal banyak file karena service pack sudah menampung semua file-file patch kecil menjadi satu.

Setiap sistem operasi Windows biasanya merilis service pack setelah beberapa saat dari rilis utamanya. Nantinya, service pack tersebut akan diberi seri seperti SP1, SP2, dan seterusnya. SP ini selain menampung perbaikan, juga menambahkan fitur baru di Windows.

Sifat service pack sendiri ada 2, yang pertama adalah inkremen, artinya updatenya baru dan belum ada di service pack sebelumnya. Sementara yang kedua adalah kumulatif, di mana update yang baru sudah ada di versi SP sebelumnya.

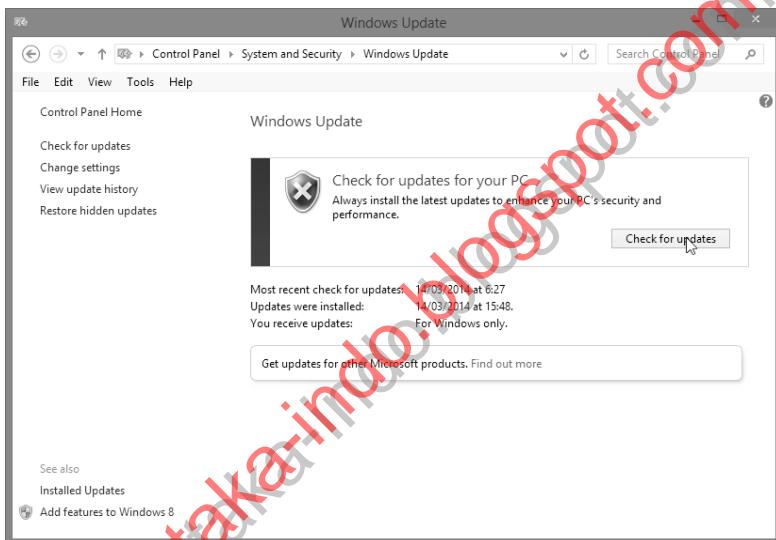
Di Microsoft, 2 sifat tersebut memiliki nama rilis yang berbeda. Rilis yang sifatnya inkremen disebut service release, sehingga ketika hendak menginstal SP2, orang harus menginstal SP1 terlebih dahulu.

Ada pengkhususan di versi Windows XP SP 3 yang sifatnya adalah SP kumulatif. Adapun, SP di Windows Vista umumnya tidak kumulatif dan inkremen. Untuk Windows 7 dan 8, istilah service pack sudah tidak ada, dan diganti dengan Windows Update.

## 4.4 Windows Update

Windows Update merupakan layanan yang disediakan oleh Microsoft yang menyediakan update (patch) untuk sistem operasi Microsoft Windows. Windows Update ini merupakan fitur yang dimiliki oleh semua versi Windows dan merupakan jalan keluar untuk menanggulangi masalah keamanan yang muncul belakangan setelah Windows tersebut dirilis.

Di Windows Vista, Windows Seven, dan Windows 8, Anda dapat mengakses Windows Update dari **Control Panel > System and Security > Windows Update**.



Gambar 4.1 Windows Update di Microsoft Windows

[pustaka-indo.blogspot.com](http://pustaka-indo.blogspot.com)

## BAB

# 5

# Email dan Ancamannya

Email merupakan sebuah fitur yang kemungkinan besar pasti digunakan oleh semua orang. Email adalah surat elektronik, yang memungkinkan semua orang saling berkirim pesan via jaringan internet. Keunggulan email adalah mudah dan bisa diakses di manapun juga.

## 5.1 Simple Mail Transfer Protocol (SMTP)

Protokol layanan SMTP berguna sebagai metode terstandarisasi untuk mengirimkan surat elektronik atau email. SMTP didesain untuk memungkinkan transfer email secara handal dan efisien.

SMTP sifatnya terbuka, jadi tidak tergantung kepada jenis komputer dan sistem operasi yang digunakan. Cara kerja SMTP adalah dengan membuat jalur antara pengirim dan penerima. Setelah jalur transmisi dibuat, barulah pengirim email akan memicu perintah MAIL yang akan mengirimkan email dengan cara mengidentifikasi pengirim dan kondisi apakah ada lalu lintas untuk dikirim.

Jika ternyata penerima dapat menerima kiriman email, maka pengirim akan memicu perintah RCPT yang fungsinya untuk mengenali penerima email. Jika penerima email dapat menerima email tersebut, maka penerima akan mengeksekusi perintah OK, dan jika tidak bisa maka akan menolaknya.

Jika penerima SMTP sudah sukses dalam memproses data email, maka SMTP akan menerima balasan OK. Email yang tidak bisa dikirim karena alamat tujuan yang salah akan dikirim balik dengan catatan dari mail server bahwa pengiriman tidak bisa dilakukan karena alasan tertentu.

Email kini sudah merupakan media penting untuk bisnis. Walaupun SMTP terbukti handal, namun sebenarnya ada kelemahannya. Email ditransfer dalam kondisi polos, artinya komputer host yang menjadi pos me-relay email dapat mengakess semua email yang melewatiinya. Sehingga, email seseorang dapat disalin atau dimodifikasi dalam perjalanan pengirimannya.

Ketika seorang yang berniat jahat menyadari bahwa admin salah satu SMTP server curiga, maka mudah sekali untuk memotong jalur email agar tidak ketahuan.

Jika ada gangguan atau upaya serangan terhadap email, maka proses pengiriman email kemungkinan dapat terhambat. Namun, ini tidak perlu dikhawatirkan karena protokol SMTP cukup kuat dan memiliki sifat untuk bisa menyembuhkan diri sendiri.

Salah satu penyalahgunaan email juga adalah orang bisa membuat pesan yang seolah dikirim dari seseorang yang lain dan bukan pengirim aslinya. Ini umumnya digunakan untuk keperluan spamming, internet marketing, dan penipuan. Bisa juga digunakan untuk merepotkan orang lain atau memfitnah. Orang yang alamatnya dibajak akan dibanjiri pesan yang mengganggu. Bisa jadi dimarahi atau diomeli orang.

## 5.2 Spam

Spam adalah ancaman paling nyata di dunia per-email-an. Banyak sekali kerugian yang diakibatkan oleh penyalahgunaan email dalam bentuk spam. Spam dimungkinkan karena biaya dan kemudahan untuk mengirim email ke banyak orang sekaligus, semudah mengirim email ke satu orang.

Di samping itu, karena seseorang bisa dengan mudah memalsukan alamat pengiriman email, maka ia dapat dengan mudah mengirim pesan ke banyak orang tanpa merasa khawatir karena alamatnya menggunakan alamat orang lain.

Email-email seperti itu disebut email spam atau email junk/sampah. Jumlahnya tak main-main. Menurut penyelidikan, hampir 50% dari lalu-lintas email yang beredar di dunia adalah spam.

Alamat-alamat email yang valid dari alamat spam ada yang dijualbelikan di sindikat spammer. Sehingga, proses spamming ini akan terus berjalan.

### 5.2.1 Mencegah Spam

Bagaimana cara mencegahnya, yang terbaik adalah memanfaatkan fasilitas antispam di email client yang Anda gunakan untuk melihat email Anda, sehingga Anda tidak perlu membuka email spam tersebut yang bisa jadi mengandung malware. Adapun jika menggunakan layanan email gratisan, Anda dapat memanfaatkan fasilitas pelaporan spam jika mendapati email spam di account email Anda.

Spam sebenarnya hanya dilakukan oleh segelintir orang saja. Namun, menjadi masalah yang amat pelik bagi sebagian besar pengguna internet. Upaya untuk memerangi spam sudah dilaksanakan sejak lama. Dan kelebihannya, tiap orang tidak dapat secara aktif menolak spam, karena hanya ISP dan pengelola mail server yang dapat mencegah spam.

Berikut ini beberapa langkah untuk mencegah atau mengurangi akibat buruk dari spam email:

- Secara pribadi, usahakan untuk tidak pernah membuka atau membalas pesan spam. Langsung saja delete, karena jika mengandung virus atau malware, jika dibuka akan membuat virus, worm, atau malware diaktifkan. Jika Anda mengenal ISP yang menjadi domain dari pengirim email, maka Anda bisa komplain ke ISP tersebut. Jika Anda berharap bahwa membalas email dan meminta pengirim untuk menghentikan email, maka ini justru akan menambah jumlah spam ke alamat email Anda.
- Beberapa negara memiliki undang-undang teknologi informasi yang mengatur spam. Anda bisa melaporkan atau memberi dukungan pada organisasi yang menangani kampanye anti spam. Di Indonesia, ini sepertinya belum begitu berjalan. Walaupun UU ITE sudah disahkan.

- Jika Anda menerima spam yang berpotensi kriminal, maka Anda bisa melaporkannya ke Departemen hukum dan HAM.
- Anda bisa melaporkan ke situs-situs yang menerima pelaporan spam, seperti [spamcop.com](http://spamcop.com), dan sebagainya.

### 5.2.2 Cara Spammer Memperoleh Alamat Email

Untuk menghindari dari spam, Anda perlu terlebih dahulu belajar bagaimana cara spammer memperoleh alamat email. Sehingga, ketika Anda mengetahui cara kerja spammer, Anda dapat dengan mudah melakukan tindakan preventif untuk spammer.

Berikut ini beberapa cara yang bisa digunakan oleh spammer untuk memperoleh alamat email:

- Dari milis: Spammer biasanya menjalankan program bot seperti yang biasa dipakai oleh mesin pencari seperti Yahoo! atau Google. Namun, data yang akan dikumpulkan hanya beberapa item, seperti header dari artikel yang mengandung alamat email, seperti Reply-To, From, dan sebagainya. Bot yang dimiliki spammer juga kadang memindai bagian isi artikel, terutama yang mengandung karakter "@" karena itu menandakan alamat email. Karena itu yang perlu Anda lakukan untuk menanggulangi hal ini adalah dengan menuliskan alamat email tidak menggunakan "@" tapi menggunakan karakter lain atau misalnya menggantinya dengan "at". Contohnya, Anda jangan menulis email Anda dengan "emailku@domainku.net" tapi "emailku[at]domainku[dot]net".
- Dari halaman web: Bot yang dimiliki scanner juga akan menjelajahi halaman-halaman web seperti halnya bot Google atau Yahoo!. Mereka akan mencari tahu alamat email di halaman web, misalnya yang berada setelah kode MAILTO di HTML. Cara untuk menanggulangi hal ini sama seperti sebelumnya, yaitu dengan tidak menuliskan "@", selain itu dengan menuliskan email menggunakan script JavaScript yang tidak bisa diparsing oleh bot dari spammer.

- Dari form web: Beberapa situs memungkinkan pengunjung untuk memasukkan data dan mengirimkan ke server menggunakan form. Kadang, di antara form itu ada kotak isian email. Nah, alamat email ini bisa diambil oleh spammer dengan 2 cara, pertama adalah karena alamat email ini ditampilkan kembali oleh website yang bersangkutan, sehingga bisa dipindai oleh bot dari spammer. Atau yang kedua adalah karena pemilik situs menjual alamat email ke spammer. Makanya, ketika Anda hendak mengisikan alamat email, pastikan Anda melakukannya di website yang dapat dipercaya. Jika tidak, lebih baik Anda mengisikan alamat email palsu atau tak perlu mengisikan alamat email.
- Cara Manual: Spammer mencatat nama email yang dilihatnya di kertas, laporan, dan sebagainya.
- Dari Contact name sebuah domain: Ketika Anda membeli domain atau hosting, Anda diminta untuk memasukkan email Anda sebagai penanggung jawab domain tersebut. Nah, spammer dapat mengetahui alamat email tersebut dengan secara manual mencatatnya di komputer.
- Menggunakan daemon: Beberapa komputer berbasis Unix menggunakan daemon (program yang berjalan di latar belakang) yang fungsinya membuat komputer dapat mengetahui siapa yang terhubung ke komputer tersebut. Daemon ini bisa mendapatkan alamat email.
- Dari web browser: Beberapa situs bisa mencuri data dari orang-orang yang membuka halaman webnya dengan cara mengambil data dari browser yang digunakannya, tanpa disadari oleh pengguna browser tersebut. Teknik yang dipakai biasanya berupa penggunaan JavaScript yang melakukan pengiriman email secara otomatis. Yang kedua menggunakan kode yang memaksa browser mengambil halaman lain di server menggunakan FTP anonim. Beberapa browser otomatis akan memberikan alamat email jika melakukan koneksi FTP anonim. Maka, alamat email tersebut akan diambil oleh server, tanpa sepengetahuan pengguna browser. Pencegahannya adalah dengan menggunakan browser yang baru, dan terkenal keandalannya.

Untuk IE, jangan gunakan IE 6, tapi gunakan versi 7 atau setelahnya. Teknik ketiga adalah menggunakan header HTTP\_FROM yang memaksa browser untuk mengirim data ke server. Untuk mengecek apakah browser yang dipakai aman atau tidak, Anda bisa mengecek melalui <http://www.cs.rochester.edu/u/ferguson/BrowserCheck.cgi>.

- Dari IRC dan chat room: Beberapa software IRC client mensyaratkan email ketika hendak bergabung. Beberapa software milik spammer bisa mengekstrak email dari software-software IRC terkenal, seperti mIRC dan sebagainya. Selain itu, ada IRCbots yang pura-pura login ke IRC dan kemudian memindai teks yang ada di room apakah ada alamat email atau tidak. Karena itu, berhati-hatilah ketika mengisikan alamat email ketika chat di IRC.
- Dari profile Yahoo!, Google, Facebook, Friendster: Hati-hati ketika menuliskan email dari layanan social networking, karena spammer senang memindai profile Anda dari Yahoo!, Google, AOL, Facebook, Friendster, Multiply, dan sebagainya.
- Dengan menebak: Bisa jadi spammer akan mengirim email coba-coba ke alamat tertentu, jika ternyata tidak ada balasan, berarti alamat email tersebut valid dan akan dikirim email terus-menerus. Cara lain untuk menentukan apakah email yang dikirim benar-benar valid adalah dengan mengirimkan "HTML email", yaitu sebuah email yang isinya kode HTML, di kode itu ada kode yang bertugas menampilkan halaman web. Ketika email tersebut dibuka, maka server tempat terletaknya gambar tersebut akan mencatat alamat email melalui log yang ada di server. Cara menebak yang kemungkinan besar tepat adalah dengan merangkai nama awal + nama akhir seseorang dan diikuti dengan @ dan ditambah nama domain dan ekstensinya.
- Dari Yellow pages: Spammer umumnya melihat calon email spammer dari perusahaan yang bonafid, caranya biasanya dengan melihat yellow pages atau layanan iklan lainnya. Ini merupakan cara manual karena itu tidak ada cara untuk mencegahnya.

- Dengan social engineering: Spammer akan mengirim surat ke sembarang alamat email dan seolah-olah dari institusi yang valid.
- Dari email dan addressbook yang terdaftar di email client, ini dilakukan dengan menggunakan virus dan worm.
- Membeli daftar email dari pemilik website besar atau dari sesama spammer. Pencegahannya adalah dengan berhati-hati ketika memberikan email di website yang tak bonafide.
- Dengan hacking: Misalnya spammer meng-hack situs Gmail dan mendapatkan alamat-alamat email, atau bisa juga menghack account administrator dari sebuah domain untuk mengetahui email-email yang ada di dalam domain tersebut. Pencegahan hal ini adalah dengan memperkuat website Anda, sehingga tidak mudah di-hack.

### 5.3 Tips Menghindari Spam

Setelah mengetahui cara kerja spammer di atas, Anda mulai dapat merumuskan beberapa tip untuk menghindari spam, antara lain:

- Hati-hati menggunakan email: Jangan gunakan email utama Anda untuk semua hal, terutama ketika menggunakan internet. Buatlah email cadangan yang bisa Anda buat memanfaatkan penyedia email gratisan yang akan disebutkan di bagian bawah bab ini. Gunakan email utama Anda (umumnya dengan domain sendiri) hanya di saat-saat tertentu, itupun harus di-masking dengan karakter yang tidak memakai "@".
- Hati-hati memasukkan data di form: Ketika memasukkan form, biasanya ada pemberitahuan di checkbox yang berisi "*YES, I want to be contacted by select third parties concerning products I might be interested in.*". Hati-hati, ini bisa saja merupakan undangan untuk spammer.
- Samarkan alamat email ketika melakukan chatting, berkomentar di blog, newsgroup, milis, dan sebagainya.

- Gunakan alamat email yang cukup panjang, misalnya jangan hanya nama depan + nama belakang, tapi tambah pula dengan inisial, umur, dan sebagainya. Semakin panjang alamat email, semakin sulit untuk ditebak dan di-spam.
- Set email yang nyasar agar tak di-forward ke root email.

Ketika sudah terlanjur menerima email sampah, Anda dapat melakukan pelaporan ke spamicop.net. Spammer umumnya dari AS, jadi ketika Anda melaporkan ke Spamicop.net, maka spammer bisa kehilangan akses internet untuk melakukan spamming dan dituntut secara hukum di negara Amerika sono.

Untuk melakukan pelaporan ke spamicop, Anda perlu menyalin isi dari email kemudian membuka situs spamicop.net, lalu register terlebih dahulu dan tempelkan isi email yang sudah disalin ke dalamnya field input yang disediakan.

## 5.4 Menggunakan Email Gratisan

Di bagian 5.3 dijelaskan bahwa salah satu teknik meminimalisasi efek spam bagi Anda adalah dengan menggunakan email utama hanya pada kondisi yang penting. Sementara untuk milis, berkomentar di blog, dan yang terekspose secara luas di internet, sebaiknya menggunakan email gratisan. Email gratisan zaman sekarang kapasitasnya sangat besar, kadang bahkan lebih besar dari email utama Anda yang didapat dari hosting berbayar.

Berikut ini beberapa penyedia layanan email gratisan yang bisa Anda coba:

- Gmail (Google Mail): Ini merupakan layanan email dari Google yang mengakomodasi email sekaligus chat. Kapasitasnya sangat banyak, sehingga Anda tidak perlu menghapus email yang sudah dimasukkan di dalamnya. Keunggulan yang lain adalah adanya akomodasi POP dan IMAP yang memungkinkan email di Gmail diambil menggunakan software mail client. Ada satu catatan tentang Gmail, yaitu Gmail menampilkan email AdSense di account email Anda. Gmail dapat diakses dari <http://mail.google.com>.

- AIM Mail: Layanan ini menyediakan kapasitas simpan yang tak terbatas, fasilitas perlindungan spam juga bagus. Keunggulan lainnya adalah adanya IMAP dan POP. Layanan ini bisa diakses dari <http://webmail.aol.com>.
- GMX Mail: Layanan ini cukup baik, kapasitasnya sekitar 5GB dan memiliki akses POP dan IMAP, sehingga bisa di-download menggunakan email client. Alamat dari gmx mail ini adalah di <http://gmx.com>. Fiturnya antara lain perlindungan terhadap virus dan spam.
- Yahoo! Mail: Ini merupakan layanan email yang cukup banyak penggunanya di Indonesia. Yahoo! Mail dapat diperoleh dengan account Yahoo! dan fiturnya antara lain kapasitas simpan yang luas, SMS, dan integrasi dengan Instant Messaging bernama Yahoo! Menssenger. Fitur lainnya adalah spam filter dan otomatis memasukkan email sampah ke junk mail. Yahoo! mail dapat diakses dari <http://mail.yahoo.com>.
- Zenbe: Zenbe adalah alternatif penyedia email yang cukup unik dalam penataannya. Ada juga fasilitas label dan pencarian email. Selain itu diintegrasikan dengan kalender, twitter, dan update facebook. Fokus dari mail ini adalah simpel dan elegan. Di sini tersedia berbagai shortcut dan punya spam filter. Akses IMAP juga ada. Anda bisa memerolehnya dari <http://www.zenbe.com>.
- Gawab.com: Gawab adalah penyedia layanan email yang cepat, stabil, dan dengan kapasitas penyimpanan 10GB. Ada juga akses IMAP. Anda bisa mendapatkan gawab dari <http://gawab.com>.
- Inbox.com: Kapasitas email dari inbox.com adalah 5 GB. Fiturnya adalah tampilan yang cantik, cepat, dan mengakmodasi POP, walaupun IMAP tidak bisa digunakan.
- Windows Live Hotmail: Layanan email gratisan yang disediakan oleh Microsoft. Fasilitasnya adalah kapasitas 5 GB, pencarian mudah dan cepat, aman, dan antarmuka yang mirip program email client, sehingga user friendly. Hanya saja tidak ada POP dan IMAP. Layanan hotmail ini dapat diakses dari <http://hotmail.com>.

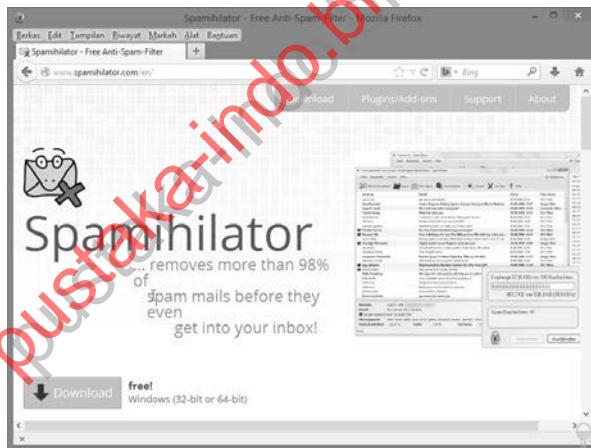
## 5.5 Menggunakan Spam Filter

Salah satu teknik untuk mempermudah Anda dalam memfilter mana yang spam dan mana yang tidak adalah menggunakan spam filter. Spam filter adalah antarmuka antara email client Anda dan server email. Jadi, Anda hanya dapat memakai software spam filter jika menggunakan software mail client dan bukan ketika mengakses via web langsung.

Beberapa software email client, misalnya seperti:

- Eudora
- Foxmail
- Microsoft Office Outlook
- Mozilla Thunderbird

Salah satu software spam filter yang free adalah Spamihilator. Silakan Anda download di [www.spamihilator.com](http://www.spamihilator.com). Sebelum menginstal software ini, pastikan software client (seperti Outlook atau Thunderbird) sudah terinstal dan account email sudah terbuat.



Gambar 5.1 Situs Spamihilator

Setelah itu, lakukan instalasi terlebih dahulu dengan cara seperti berikut ini:

1. Eksekusi file installer spamihilator dan kemudian klik button **Next** di **Welcome to the Spamihilator Setup Wizard**.



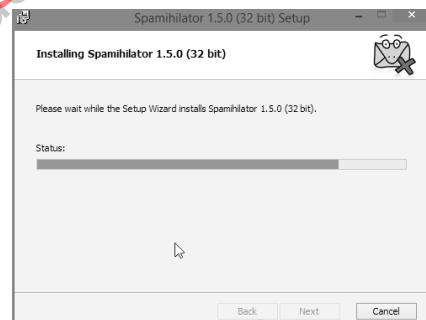
*Gambar 5.2 Jendela Welcome to the Spamihilator Setup Wizard*

2. Di **License Agreement**, klik button **I agree**. Licensi dari Spamihilator adalah free walaupun tidak open source.



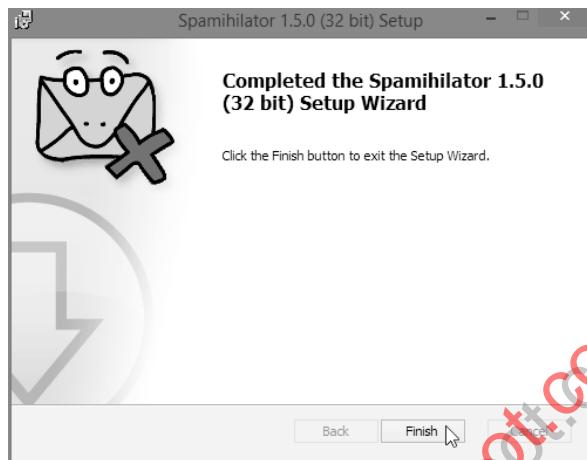
*Gambar 5.3 Jendela License Agreement Spamihilator*

3. Tunggu hingga instalasi selesai.



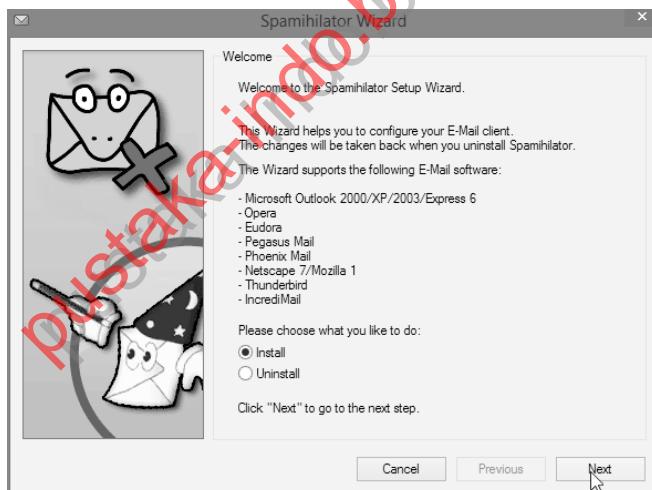
*Gambar 5.4 Instalasi komponen utama dan plugin dari spamihilator*

4. Kalau instalasi sudah selesai, muncul **Completed the Spamihilator Setup Wizard**, klik **Finish**.



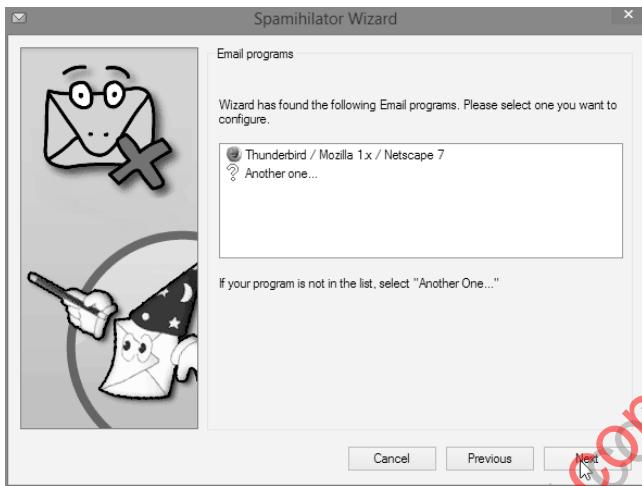
*Gambar 5.5 Jendela Completed the Spamihilator Setup wizard*

5. Maka muncul wizard spamihilator, klik **Install** dan pilih **Next**.



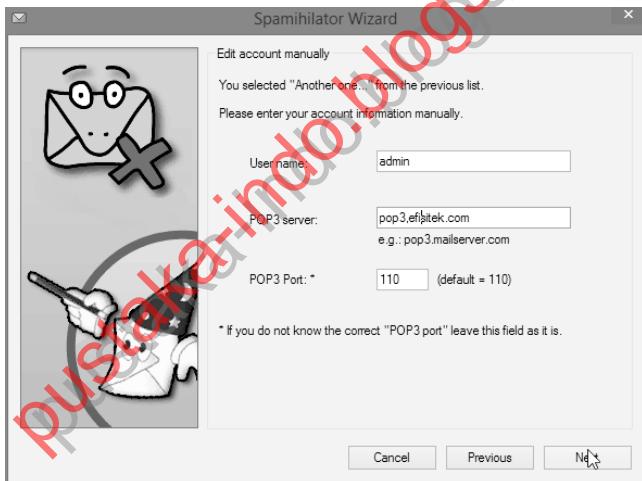
*Gambar 5.6 Klik Install dan Next*

6. Pilih email program yang Anda miliki dan klik **Next**.



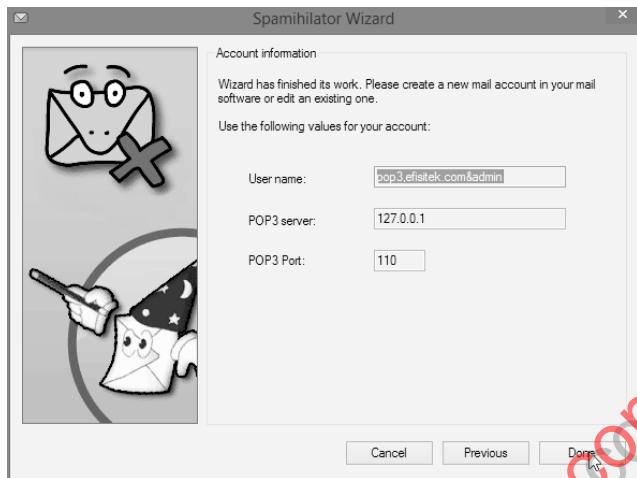
Gambar 5.7 Pemilihan program email

7. Isikan username, nama server POP3 dan port POP3.



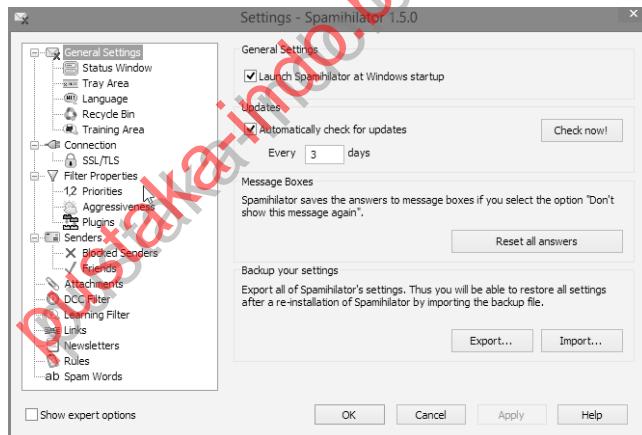
Gambar 5.8 Pengisian username, server pop3, dan port pop3

8. Di Account information, Anda bisa mengecek apakah informasi sudah benar.



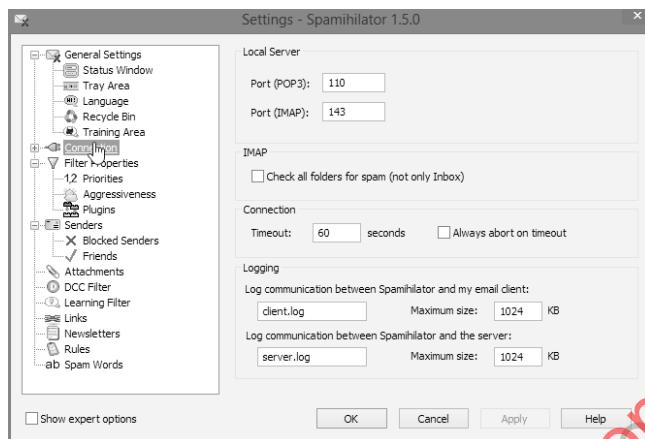
Gambar 5.9 Konfirmasi apakah akun informasi sudah benar

9. Anda bisa menyetting spamihilator agar optimal. Di **General Settings**, terlihat opsi apakah aplikasi ini dijalankan saat startup, lalu apakah akan diupdate secara otomatis.



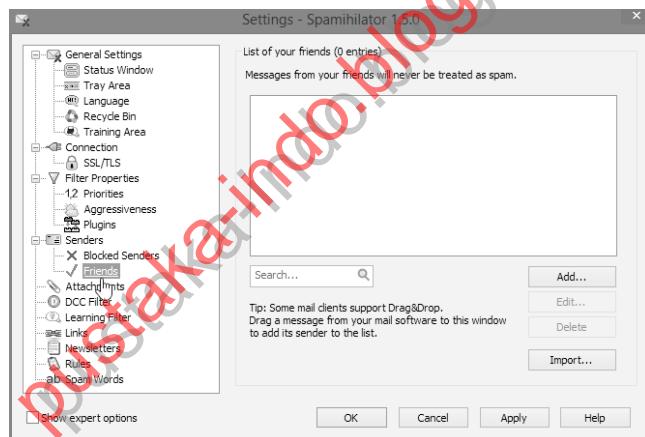
Gambar 5.10 Pengaturan tab General

10. Di **Connection**, Anda bisa mengatur port POP3, IMAP, dan timeout untuk memutuskan koneksi.



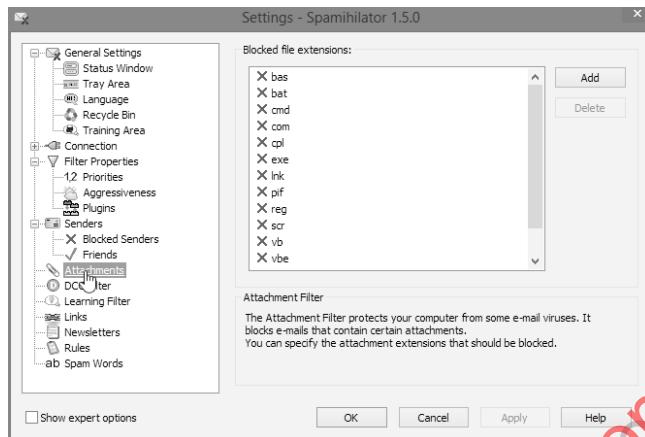
Gambar 5.11 Pengaturan tab Connections

11. Di **Senders > Friends**, Anda bisa memasukkan whitelist yang membuat pesan dari sender ini akan selalu diterima dan tidak pernah dianggap spam.



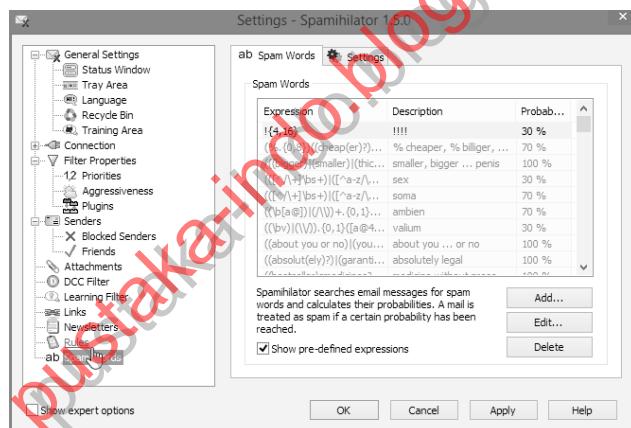
Gambar 5.12 Pengaturan Sender

12. Di **Attachments**, Anda bisa menambahkan ekstensi file attachment yang akan dianggap sebagai attachment.



Gambar 5.13 Ekstensi file attachment

13. Di **Spam Words**, Anda bisa memasukkan ekspresi yang menjelaskan kata-kata yang apabila ditemui di spam words, akan diblokir.



Gambar 5.14 Spam words

## BAB

# 6

# Backup dan Restore

Backup atau menyimpan konfigurasi komputer dalam suatu kondisi normal dengan harapan bisa dikembalikan lagi/restore adalah salah satu teknik konvensional dan kuratif dalam hal penjagaan keamanan komputer. Walaupun sepele, tapi backup merupakan andalan terakhir ketika semua cara untuk mengembalikan komputer ke kondisi sehat tidak berhasil.

## 6.1 Backup MBR

*Master Boot Record (MBR)* adalah komponen kecil yang terletak di awal sebuah harddisk. MBR berguna menyimpan informasi boot dan layout partisi untuk semua disk. MBR sendiri hanya berupa satu sektor fisik berukuran 512 byte.

Walaupun teramat kecil ukurannya, namun fungsinya sangatlah penting. MBR diperlukan untuk membuat atau menjaga partisi di harddisk dan juga untuk keperluan booting komputer.

Saat bagian tertentu dari MBR hilang atau corrupt, maka komputer tidak akan bisa booting. Misalnya, ketika tabel partisi tidak diisi dengan informasi partisi yang benar, maka tidak hanya boot loader yang tidak bisa identifikasi partisi mana yang harus di-booting, namun juga partisi dan semua file di dalamnya akan hilang.

Begitu pula jika kode boot loader tidak konsisten atau corrupt, maka proses booting tidak bisa dijalankan dan komputer tidak akan bisa dioperasikan karena tidak bisa melakukan booting ke sistem operasi tertentu.

Apa yang menyebabkan kerusakan MBR? Penyebabnya antara lain virus yang menyerang boot sector. Beberapa virus yang menyerang boot sector bisa mengubah dan merusak MBR dan label volume dari hard disk. Karena itulah backup MBR penting.

Untuk membackup MBR, Anda harus menggunakan tool eksternal karena tidak ada fitur bawaan dari Windows untuk backup MBR.

### 6.1.1 HDHacker

HDHacker yang bisa diambil dari situs HDHacker merupakan tool backup untuk Windows yang memungkinkan Anda menyimpan, melihat, dan me-restore MBR, boot sector atau sembarang sector di hard disk. Tidak hanya itu, sebenarnya HDHacker juga bisa dipakai untuk floppy disk, memory stick, dan semua media lainnya.

Yang membuat software ini sangat berguna adalah karena sifatnya yang free. Selain itu, software ini stand alone, sehingga tidak perlu diinstal dan hanya menggunakan satu file executable.

Berikut ini contoh beberapa skenario kapan Anda dapat menggunakan software HDHacker untuk memproteksi MBR:

- Jika PC rawan terserang virus boot sector.
- Jika PC memiliki multi sistem operasi, seperti Windows dan Linux. HDHacker bisa dipakai untuk membackup MBR, sehingga jika LILO atau GRUB yang merupakan boot loader di Linux tertimpa ketika Anda melakukan instal ulang, LILO atau Grub tersebut masih bisa dipulihkan kembali. Lakukan backup sebelum Anda menginstal ulang Windows.

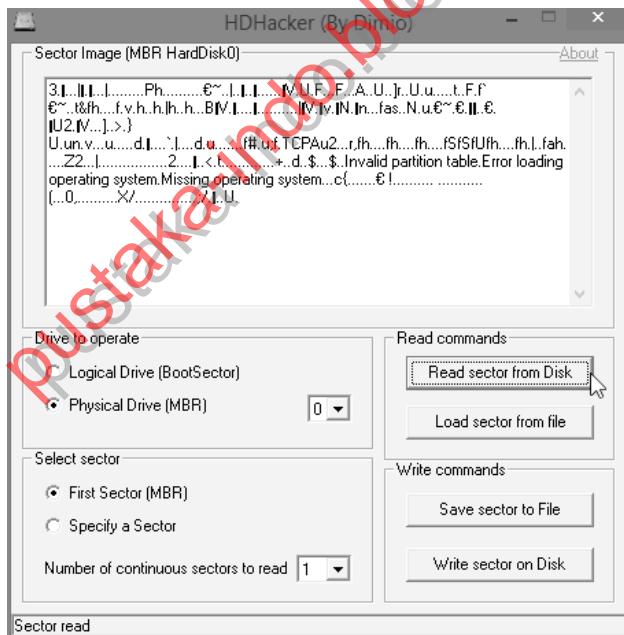
Software HDHacker memungkinkan Anda untuk membaca, menulis dari dan ke drive fisik. Jika sektor pertama dipilih di drive fisik, maka artinya itulah MBR. Sementara, jika sektor pertama dipilih di drive logis, maka yang diacu adalah boot untuk sektor tersebut.

Jadi MBR bisa digunakan untuk melakukan operasi berikut:

- **Read Sector From Disk:** Memuat informasi sektor ke memory, yang sebelumnya sudah dibaca dari disk.
- **Load Sector From File:** Memuat sektor ke memory, yang sebelumnya sudah disimpan ke file.
- **Save Sector To File:** Menyimpan sektor di memory ke file atau ke media atau disk tertentu.
- **Write Sector On Disk:** Menuliskan sektor di memory ke disk, di bagian lokasi MBR atau boot sektor.

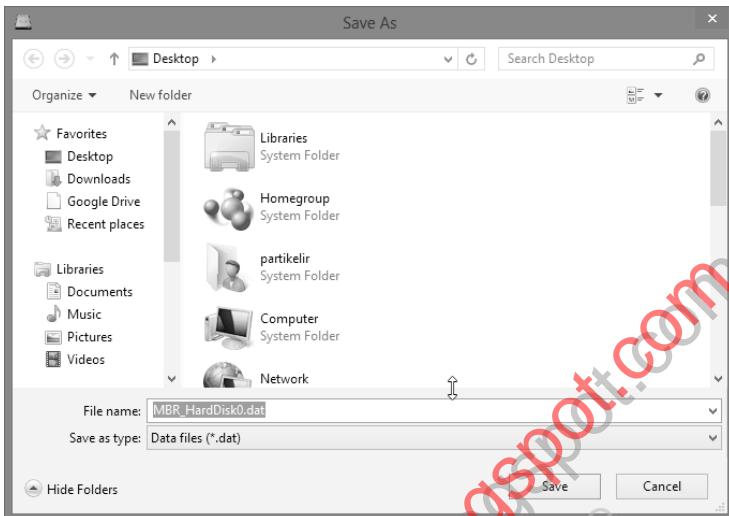
Ketika Anda hendak menyimpan data MBR (atau dengan kata lain mem-backup MBR), Anda dapat melakukan langkah berikut ini:

1. Pilih drive fisik.
2. Lalu pilih combobox 0 di samping kanan
3. Klik button **Read Sector From Disk**.
4. Untuk menyimpan, klik **Save Sector To File**.



Gambar 6.1 MBR dilihat dan siap untuk disimpan ke file

5. Kemudian, tentukan lokasi file penyimpanan di window **Save As**. Klik **Save**, maka file akan tersimpan. File MBR akan disimpan ke dalam format file .dat.

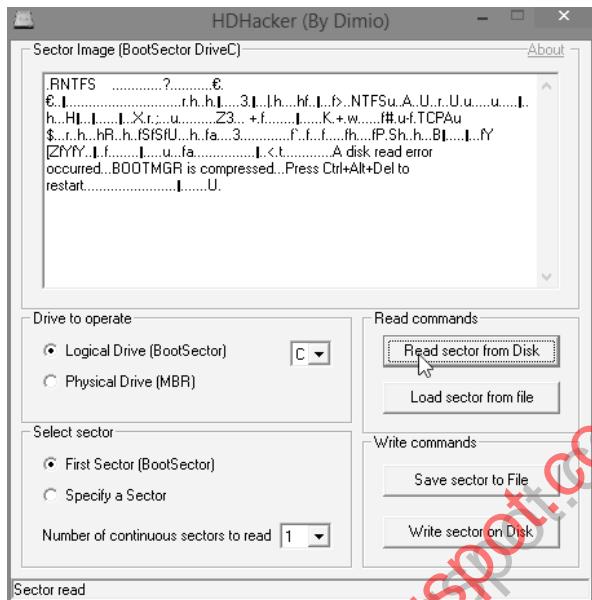


*Gambar 6.2 Memilih lokasi penyimpanan file*

Langkah-langkah di atas dilakukan jika Anda ingin menyimpan MBR pada file tertentu. Adapun untuk me-restore, Anda dapat melakukan langkah berikut:

1. Pilih drive fisik yang akan di-restore.
2. Klik button **Load Sector From File**. Kemudian, cari file backup yang telah disimpan sebelumnya.
3. Pilih **Write Sector On Disk** untuk menerapkan penulisan MBR.

HDHacker dapat diterapkan di semua versi Windows. Tidak hanya MBR, HDHacker juga dapat digunakan untuk membaca bagian logis dari sektor tertentu di hard disk. Anda hanya tinggal memilih Logical drive di groupbox **Drive to operate**, dan memilih sektornya di groupbox **Select Sector**.



Gambar 6.3 Membaca sektor dari drive logis dengan HDHacker

### 6.1.2 MBR Wiz

MBRWiz dari <http://firesage.com/mbrwizard.php> ini bisa melakukan banyak hal, yang dibagi dalam 3 golongan, yaitu fungsi editing MBR, partisi, dan fungsi tambahan. Untuk editing MBR, Anda dapat melakukan hal berikut ini:

- Save atau Backup MBR.
- Restore MBR dari backup.
- Menghapus MBR tertentu.
- Memperbaiki MBR yang corrupt.
- Membuat MBR baru.
- Memodifikasi signature dari disk.
- Menyortir entri dari tabel partisi.
- Menyalin sektor.
- Menghapus MBR yang ada sekarang.

Untuk partisi, MBRWiz dapat melakukan hal berikut:

- Menghapus partisi.
- Menyembunyikan/menampakkan partisi.
- Menyeting partisi agar bootable/aktif.
- Mengganti tipe partisi.

Fitur tambahan dari MBRWiz adalah:

- Melakukan penghapusan disk secara keseluruhan dengan aman.
- Memilih partisi yang bootable di boot menu.
- Memelihara byte status agar konsisten.
- Membuat file .ini yang berisi MBR.
- Melakukan shutdown dan reboot.

MBRWiz adalah tool berbasis DOS, sehingga cocok digunakan via jaringan, misalnya via telnet.

Untuk meminta MBRWiz melakukan sesuatu, Anda tinggal mengakses file mbrwiz.exe dan ditambah dengan operator yang diinginkan. Misalnya, untuk mengetahui daftar partisi yang terdaftar di MBR, Anda bisa mengeksekusi perintah:

```
C:\lokasi_file\mbrwiz.exe /list
```

Hasilnya terlihat seperti berikut.

```
2 Drives > 5,376,167,936 bytes free
C:\Documents and Settings\Zuppery\Desktop\File-file security\Bab 6>MbrWiz.exe
MbrWiz - Version 2.0 ***beta*** for Windows XP/2K3/PE April 30, 2006
Copyright (c) 2002-2006 Roger Layton http://mbr.bigr.net

Invalid or incomplete switch:
C:\Documents and Settings\Zuppery\Desktop\File-file security\Bab 6>MbrWiz.exe /list
MbrWiz - Version 2.0 ***beta*** for Windows XP/2K3/PE April 30, 2006
Copyright (c) 2002-2006 Roger Layton http://mbr.bigr.net

Disk: 0 Size: 38G CHS: 4864 255 63
Pos MBRIdx Type/Name Size Active Hide Start Sector Sectors DL Vol Label
 0   0    02-NTPS  15G Yes  No      63 30,716,217 C: OS
 1   1    0F-EXTEND 23G No   No     30,716,280 47,423,880 -- <None>

C:\Documents and Settings\Zuppery\Desktop\File-file security\Bab 6>
```

Gambar 6.4 Melihat partisi yang terdaftar di MBR dengan MBRWiz

Beberapa syntax kode operasi MBRWiz ini adalah seperti berikut:

- /List - Menampilkan semua partisi yang terdaftar di MBR beserta urutannya. Ditampilkan pula tipe partisi, ukuran, apakah partisi tersebut aktif atau hidden. Field pos menunjukkan urutan partisi di disk, sementara MBRndx menunjukkan bahwa partisi terdaftar di MBR.
- /Disk=# - Memilih disk yang akan digunakan untuk semua operasi. Ini menunjukkan bahwa semua operasi yang ditentukan di command line akan menggunakan disk yang dimaksud. Jika tidak diisikan, maka nilai default adalah 0.
- /Part=# - Memilih partisi yang akan digunakan untuk operasi. Jika tidak ditentukan, maka partisi 0 akan digunakan. Semua operasi menggunakan lokasi fisik dari partisi di harddisk (kolom pertama yang terlihat jika menggunakan perintah /list). Jika ingin command diterapkan di semua partisi, gunakan kode Part=\*(asterisk).
- /Sector=# - Memilih sektor yang hendak digunakan oleh operasi MBRWiz. Jika tidak ditentukan, maka sektor 0 yang digunakan.

Untuk mengedit MBR, berikut ini beberapa kode yang digunakan:

- /Save=filename - Menyimpan MBR yang ada saat ini ke file tertentu. Inilah yang disebut backup. Parameter filename menjelaskan lokasi ditambah nama file yang dimaksud. Jika Anda memberi parameter /Sector=# di command line, maka yang disimpan sektor tersebut dan bukan MBR MBR (Sector 0).
- /Restore=filename - Membaca MBR dari file tertentu di mana nama file sama seperti /Save di atas, yaitu mengacu pada lokasi dan nama file tersebut. Ini digunakan untuk restore MBR. Jika ada parameter tambahan /Sector=# parameter maka restore akan diterapkan ke sektor tersebut dan bukan ke sektor 0 (MBR).
- /Repair=# - Membuat Master Boot Record baru di disk yang kosong, bisa digunakan untuk memperbaiki disk yang rusak, corrupt, atau kehilangan MBR. Jika nilai parameter diset ke '1', maka akan menyimpan MBR untuk Windows XP/2003 ke disk. Opsi ini tidak akan memodifikasi tabel partisi.

- /Show=x - Menunjukkan struktur partisi dari MBR yang di-backup. Opsi untuk parameter x adalah nama file, nomor sektor yang mengandung backup atau kata "SECTOR" jika isi MBR sudah disimpan ke sektor yang hidden.
- /Wipe=x - Mengisikan opsi 'mbr' akan menyebabkan MBRWiz menghapus MBR sampai bersih, 'head' akan membersihkan head pertama atau sekitar 63 sektor. Anda juga bisa menentukan jangkauan dari sektor yang ingin dihapus dengan menuliskan parameter seperti /Wipe=x-y. Ini akan menghapus semua informasi dari sektor yang ditentukan mulai sektor ke-x sampai sektor ke-y.
- /Sort - Kadang entri partisi di MBR tidak teratur setelah Anda menginstal ulang Windows atau me-restore partisi menggunakan software seperti Norton Ghost atau Acronis. Ini artinya urutan partisi di MBR tidak cocok dengan urutan di disk. Jika kebetulan Anda menggunakan Windows NT, 2000, XP, dan Vista, maka ini bisa menjadi masalah, karena itu opsi ini akan mengurutkan entri di MBR, sehingga cocok dengan urutan fisik di hard disk.
- /IsSorted - Query terhadap urutan entri partisi di MBR dan mengembalikan kode ErrorLevel berdasarkan status dari entri partisi. Nilai opsi '0' = Sorted, '1' = Not Sorted.
- /Signature=x - Membaca atau menulisi signature dari hard disk baru ke MBR. Dengan menentukan nilai "Zero", artinya Anda akan menghapus signature yang sudah ada. Adapun jika tidak, maka entry 8 digit hexadesimal bisa dimasukkan untuk signature. Contoh pengisian misalnya /Signature= Zero, atau /Signature= AC87AD87. Penentuan /Signature tanpa mengisi opsi akan menampilkan disk signature yang ada sekarang.
- /Copy=x - Menyalin isi dari satu sektor ke lokasi lainnya. Misalnya, command /Sector=x akan menentukan sektor sumber yang disalin. Dan penyalinan dilakukan dengan perintah /Copy ini. (Umumnya, sektor pertama dari 0-63 digunakan sebagai sumber. Jika target ditentukan sebagai 0, maka ini akan menimpa MBR, sehingga MBR terhapus.

MBRWiz juga dilengkapi dengan parameter command untuk mengolah partisi. Parameter tersebut adalah seperti berikut:

- /Hide=# - Menyembunyikan atau menampilkan partisi tertentu di sistem operasi. Opsi '1' artinya 'Yes', sehingga partisi akan disembunyikan. Sementara, memilih '0' atau 'No' akan membuat partisi kelihatan. Jika /Part=\*, maka semua partisi akan ditentukan sesuai dengan opsi, baik semuanya hidden atau semuanya terlihat.
- /Active=# - Menentukan partisi tertentu apakah aktif (bootable) atau tidak? Mengisikan parameter '1' atau 'Yes' akan membuat partisi tertentu aktif, sementara pengisian parameter '0' atau 'No' akan menentukan partisi tidak aktif (tidak bisa diboot). Jika /Part=\* digunakan, maka semua partisi akan diset apakah aktif atau tidak. Jika Anda ingin membuat partisi hidden yang aktif, maka pertama harus diaktifkan dalam kondisi tidak hidden kemudian di-hidden.
- /Type=# - Memodifikasi tipe partisi di MBR. Ini tidak akan mengonversi tipe partisi sistem file ke tipe yang baru. Ini umumnya diperlukan ketika program pemartisi atau backup/restore memodifikasi tipe partisi dan karenanya perlu dikembalikan lagi ke tipe aslinya. Nilai # harus diikuti oleh 'd' atau 'h'. d artinya desimal, h artinya hexadesimal. Opsi ini harus digunakan bersamaan dengan /Partition untuk menentukan identitas partisi yang dimodifikasi.
- /Del - Menghapus partisi tertentu, misalnya /Part=\* akan menghapus semua partisi yang terpilih, sementara /Disk=\* /Part=\* akan menghapus semua partisi di semua disk.

Ada opsi-opsi lain selain opsi yang telah dijelaskan di atas untuk MBRWiz, antara lain seperti berikut:

- /Shutdown=# - Jika # bernilai '1', maka Windows akan dipaksa untuk shutdown. '2' akan memaksa Windows untuk shutdown dan reboot (restart), '3' akan mematikan komputer tanpa paksaan, dan '4' akan merestart komputer tanpa paksaan. Mematikan atau merestart dengan paksaan akan menyebabkan kehilangan data jika data belum disimpan. Ini hanya bisa diterapkan di Windows NT/2K/XP/Vista dan terbaru.

- /WipeDisk=# - Akan menimpa tiap sektor di harddisk dengan data agar penghapusan benar-benar aman dan file tidak bisa direcover kembali. Menggunakan opsi '1' akan menimpa sektor dengan nilai zero. Jika dijalankan dari dalam DOS Windows, maka MBRWiz tidak bisa menghapus drive C secara komplit, karena akan muncul blue screen saat file-file sistem operasi terhapus. Jika demikian, Anda bisa boot dengan DOS dan kemudian mengakses Wipedisk dari DOS.
- /Status=x - Menyimpan atau mengambil byte status yang terletak di offset 0x1b2 di bagian MBR. Offset ini adalah sebuah section yang tidak digunakan di MBR. Dengan perintah ini, Anda bisa menyimpan satu byte di lokasi yang tidak dipakai di harddisk. Tujuannya sebagai indikator status atau apa pun. Nilai yang dimasukkan di sini bisa antara 0-255. Jika menggunakan perintah /Status tanpa opsi, maka hasilnya adalah byte tidak berubah.
- /Confirm - Operasi yang melakukan perubahan ke MBR akan meminta konfirmasi user sebelum diubah. Dengan menggunakan /confirm di command line, maka permintaan ini tidak perlu dieksekusi dan otomatis langsung dialokasikan ke Yes.
- /BootMenu - Opsi ini akan menampilkan list booting yang ada. Partisi yang bootable akan ditampilkan. Anda bisa memilih satu partisi yang aktif dengan memilih dari menu.
- /Msg=# - Menyembunyikan status pesan yang ditampilkan ketika program keluar. Nilai '1' menunjukkan tidak ada pesan yang ditampilkan, '2'=menunjukkan tidak ada pesan error, dan '3'=tidak ada pesan status yang ditampilkan jika sukses.
- /Ignore - Akan meneruskan aksi walaupun ada error terjadi.
- /Result - Menampilkan kode balikan untuk verifikasi visual apakah sukses atau tidak.
- /? - Menampilkan opsi command line.

C:\Documents and Settings\Zuperry\Desktop\File security\bab 6\MBRWiz.exe

MBRWiz - Version 2.0 \*\*beta\*\* for Windows XP/2K3/PE April 30, 2006  
Copyright <c> 2002-2006 Roger Layton http://mbr.bigr.net

Usage: MBRWiz [/option]  
/List: List MBR Entries  
/Disk:# Selects the disk to use, '0' is used if not specified  
/Part:# Specifies partition to use. Defaults to '0'  
/Sector=# Specifies sector (or sectors) to use for certain operations  
/Save=x Saves MBR to filename 'x', or first head using /Sector=head  
/Restore=x Reads and restores the MBR from filename 'x'  
/Repair=x 1=Repairs a missing or corrupt PE/XP/2K3 boot record  
/Show=x Shows contents of MBR backup file 'x'  
/Wipe=x MBR-Wipes MBR, HEAD-Wipes first head, 3-Wipes range of sectors  
/Sort Sort MBR Entries by physical location on disk  
/IsSorted Returns 0 if MBR partitions are already sorted  
/Hide=# 1=Hide partition, 0=Unhide partition  
/Active=# 1=Sets the partition bootable, 0=Set it inactive  
/Del Deletes the partition specified by /Part  
/Type=# Modifies the specified partition type to #  
/Mount=x: Mounts Volume with drive letter x:, used with /Part or /Vol  
/Unmount=x: UnMounts volume by partition #, volume label, or drive letter  
/Label=x Assigns the selected volume label as x

Press any key for remaining options...

Gambar 6.5 Penjelasan perintah MBR

## 6.2 Backup File

Kegiatan backup yang sering diperlukan sehari-hari adalah backup file atau folder tertentu. Dengan backup file, Anda akan menyimpan file untuk disimpan dan dijadikan cadangan jika file tersebut corrupt, error, dan tidak konsekuensi. Software backup membantu Anda melakukan backup karena bisa mengotomasi pemindahan file backup ke tempat tertentu secara otomatis.

### 6.2.1 Instalasi Cobian Backup

Salah satu software free dan open source terbaik untuk backup adalah Cobian Backup. Cobian Backup merupakan program multi-thread yang bisa digunakan untuk membackup dan menjadwalkan backup file atau direktori dari lokasi asli ke lokasi yang diinginkan. Tidak hanya di satu komputer, namun bisa juga di komputer jaringan atau bahkan via FTP. Cobian memiliki situs resmi di <http://www.educ.umu.se/~cobian>.

Aplikasi ini bisa dijalankan sebagai service yang berjalan di belakang (daemon) atau sebagai aplikasi biasa. Program ini cukup baik karena hanya sedikit mengonsumsi daya.

Dengan menggunakan software ini, Anda dapat backup file secara otomatis dan tiap periode tertentu, misalnya sekali saja, harian, mingguan, bulanan, tahunan atau tiap periode waktu tertentu.

Anda juga bisa menentukan apakah file backup dikompres atau tidak?

Untuk bisa menggunakan Cobian Backup, pertama kali install dahulu program tersebut seperti berikut:

1. Eksekusi file installer Cobian Backup. Muncul jendela **Welcome to Cobian Backup** seperti berikut, klik **Next**.



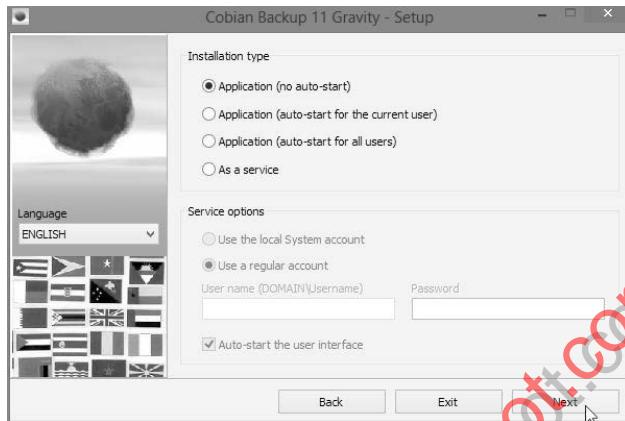
Gambar 6.6 Jendela Welcome to Cobian backup

2. Tentukan lokasi instalasi di **Installation directory**, klik **Next**.



Gambar 6.7 Penentuan Installation Directory

3. Tentukan tipe instalasi sebagai **Application no auto start**, sehingga Anda hanya perlu memanggil aplikasi ketika diperlukan saja.



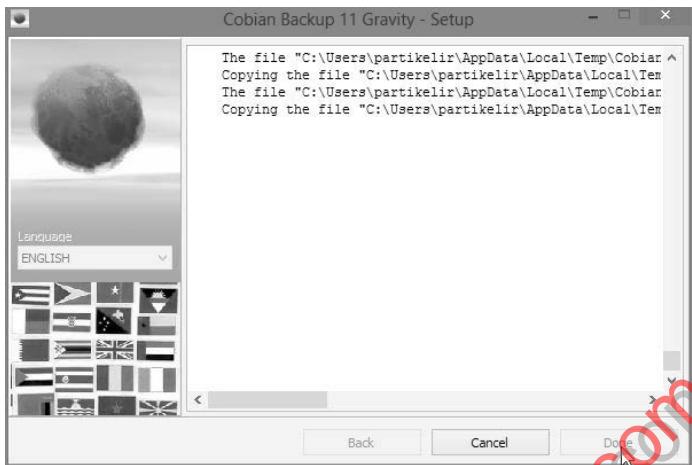
Gambar 6.8 Pengesetan sebagai Application (no auto start)

4. Kalau sudah siap menginstal, muncul jendela seperti berikut, klik tombol **Install**.



Gambar 6.9 Proses instalasi sedang berlangsung

5. Proses instalasi dilakukan, tunggu hingga selesai.

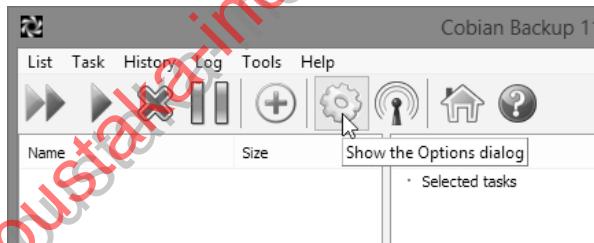


Gambar 6.10 Proses instalasi dilakukan

6. Klik Done.

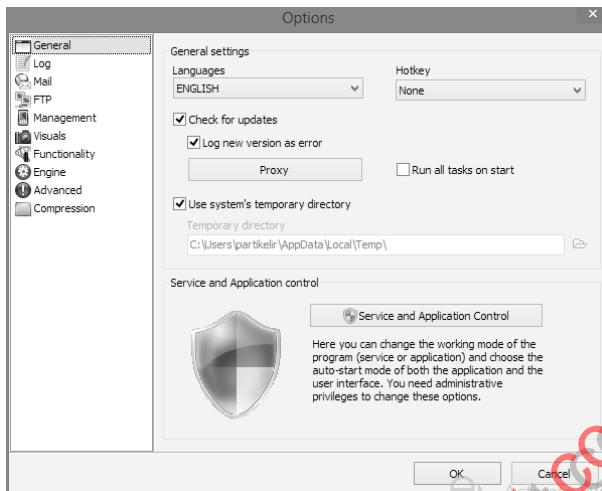
### 6.2.2 Pengaturan Opsi Cobian Backup

Setelah menginstal, saatnya Anda mengatur opsi dari Cobian Backup. Untuk mengatur, klik tombol **Open the options dialog** di toolbar seperti terlihat di gambar berikut ini.



Gambar 6.11 Tombol *Open the Options Dialog* di toolbar

Di **General**, Anda dapat memilih bahasa, shortcut hotkey, dan cek untuk update.



Gambar 6.12 Tab General di window Options

Tab pertama di window Options adalah tab **General**. Di sini, Anda melihat beberapa pengaturan. Combobox pertama adalah menentukan tipe aplikasi, di sini ada beberapa pilihan:

- **Run All task on start:** Ketika program dijalankan sebagai aplikasi, Anda dapat menentukan bagaimana program dimulai, apakah sejak Windows memulai, atau manual. Jika Cobian dijalankan sebagai service, maka hal ini tidak bisa diseting.
- **No Autostart:** Program harus dimulai dengan mengeksekusinya secara manual barulah program akan bisa aktif.
- **Autostart interface for the service:** jika program dijalankan sebagai service, Anda dapat menentukan apakah antarmuka otomatis dimulai atau di-disable.

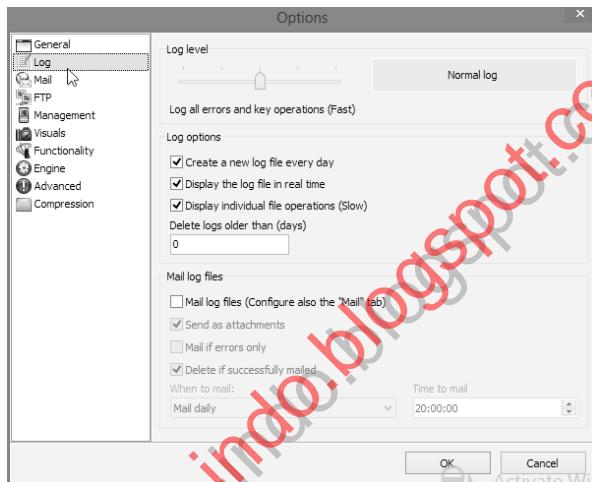
Di bagian **Service And Application Control** ada berbagai button, seperti: **Start**, **Install**, **Uninstall**, **Stop**, **Logon**. Di sini, Anda dapat mengatur service dari Cobian tanpa harus membuka Control Panel atau tanpa instal ulang program tersebut.

Jika Cobian diinstal sebagai aplikasi, dan Anda ingin mengubahnya sebagai service, maka Anda tinggal mengklik pada button **Install**. Di bawahnya ada **Language** yang mengizinkan Anda memilih bahasa untuk antarmuka Cobian.

Bagian **Temporary directory** menunjukkan lokasi direktori yang digunakan untuk operasi zip. Pastikan kapasitas folder yang ada di Temporary directory ini mencukupi. Jika tidak, Anda tidak maka proses kompresi atau enkripsi bisa gagal.

Bagian **Hotkey** menentukan apakah Anda bisa mengonfigurasi shortcut yang akan membuka jendela interface Cobian ketika shortcut tersebut ditekan.

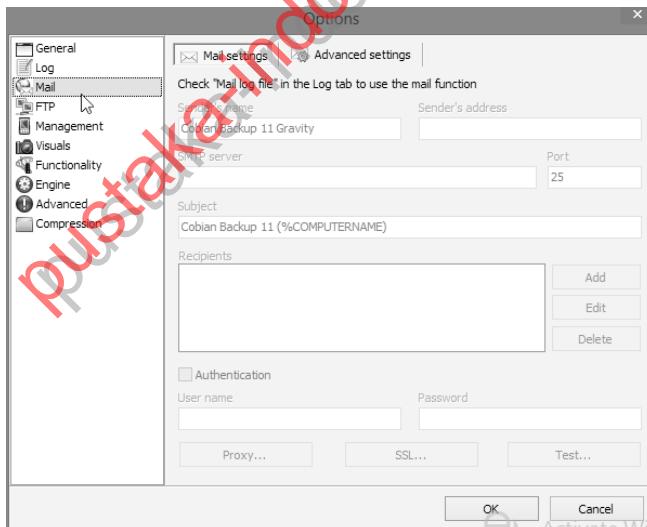
Untuk mengatur logging atau pencatatan kegiatan di Cobian, klik pada tab **Log** sehingga muncul tampilan seperti gambar berikut ini.



Gambar 6.13 Tab Log dari window Options Cobian Backup

- Bagian **Log events** (nilai asli terconteng) menentukan diciptakannya file log jika checkbox ini terconteng, sementara jika Anda tidak memerlukan file log, maka bagian ini tidak perlu diconteng.
- **Log errors only** menentukan apakah Anda ingin menambahkan entry ke log jika ada kegagalan operasi tertentu saja. Sehingga, jika tidak ada catatan, berarti operasi backup berjalan sukses.
- **Verbose** jika dicek artinya tiap operasi akan dicatat ke file log, walaupun operasi yang tidak terlalu penting. Konsekuensinya file log akan besar sekali. Ini diperlukan saat ada error dalam operasi, dan Anda ingin melakukan debug.

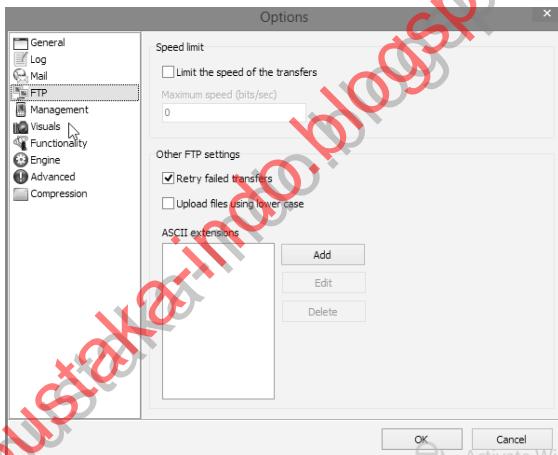
- **Show the log in real time** menunjukkan bahwa semua event yang ditambahkan ke file log akan ditunjukkan secara real time.
- **Mail log** digunakan jika Anda menjalankan Cobian Backup di komputer remote, maka Anda bisa menerima log via email menggunakan fitur ini. Jika Ya, maka Anda perlu konfigurasi SMTP server, seperti ketika mengonfigurasi mail client (Outlook atau Thunderbird).
- **Delete on mail** menentukan apabila log sudah dikirim via email, maka log di disk dihapus.
- **Send as attachment** menentukan apakah file log akan dikirim sebagai attachment yang ter-zip. Jika tidak dicek, maka file log akan dikirim sebagai teks di body email.
- **Mail if errors only** menentukan apakah Cobian akan mengirim email jika di file log ada catatan error dalam operasi. Jika tidak ada error berarti tidak akan dikirim.
- **Time to mail** menentukan waktu kapan file log dikirim.
- **Mail after backup** menentukan agar file log dikirim langsung ketika backup sudah selesai.



Gambar 6.14 Tab SMTP untuk mengatur mail log file

Ketika menyeting Mail, Anda perlu menyeting beberapa hal:

- **Sender's name:** Nama yang akan terlihat di field FROM dari pesan email yang terkirim.
- **Subject:** Teks untuk judul email.
- **Sender's address:** Alamat email untuk pengirim, beberapa SMTP memverifikasi alamat pengirim ini.
- **Server host:** Nama SMTP server yang digunakan.
- **Port:** Port SMTP yang digunakan, nilai default adalah (Default=25).
- **Recipients:** Alamat email tujuan di mana merupakan alamat untuk menerima pengiriman catatan log tersebut.
- **Password:** jika menggunakan SMTP yang secure, maka isikan password di sini.



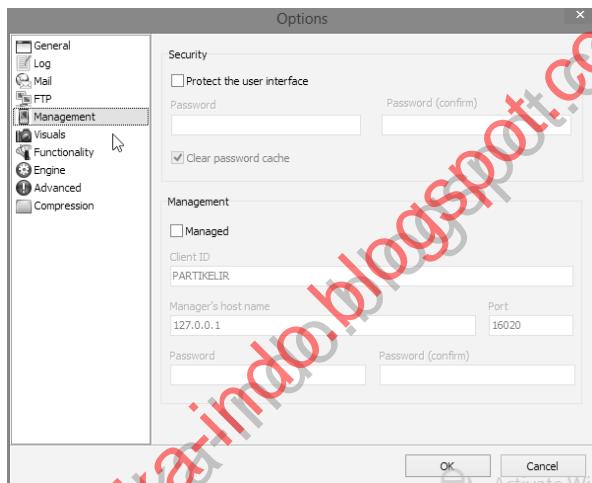
Gambar 6.15 Tab FTP

Di tab FTP, Anda bisa menentukan beberapa atribut berkaitan backup FTP. Berikut ini beberapa item dan penjelasan fungsinya:

- **Speed limit:** jika diberi cek, maka kecepatan transfer data ke FTP server akan dibatasi. Ini cocok jika Anda memiliki bandwidth terbatas. Sehingga, bandwidth untuk transfer FTP dibatasi agar tidak menyedot bandwidth yang diperlukan untuk aplikasi lainnya.

- Textbox **Speed** digunakan untuk mengisikan kecepatan yang menjadi batas maksimal dalam satuan bit per detik. Ini hanya dapat diisikan jika Anda ingin membatasi bandwidth.

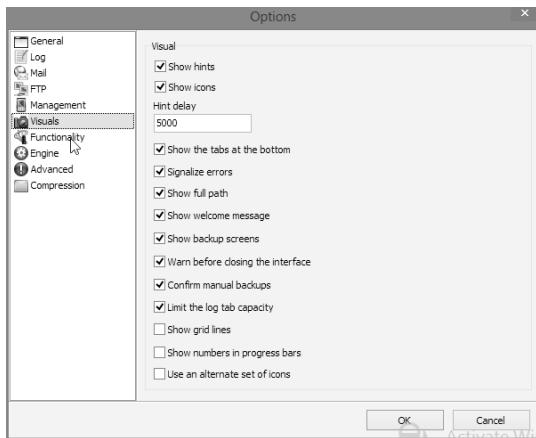
Beberapa FTP server menyimpan file biner dan file teks menggunakan cara yang berbeda-beda. Misalnya untuk file executable, terkompres, gambar, dan multimedia, metode transfer yang digunakan adalah binary transfer. Sementara untuk file teks seperti file berbasis ASCII seperti HTML TXT, maka gunakan metode ASCII transfer. Untuk itu, Anda dapat memasukkan ekstensi file-file yang ingin memakai ASCII transfer. Misalnya: .txt, .htm, .ini.



Gambar 6.16 Tab Management di Cobian Backup

Di tab **Management** Anda dapat mengatur password untuk user interface dari Cobian Backup ini. Jika ingin memproteksi, maka Anda dapat mencek pada checkbox **Protect the user interface**. Sehingga, jika user tidak mengetahui user dan password untuk membuka Cobian, maka Cobian akan tidak bisa diakses.

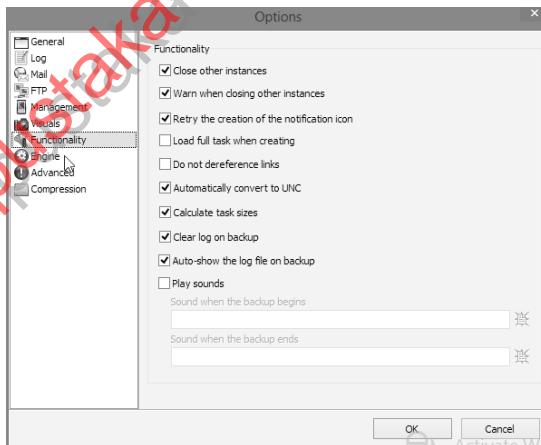
Isikan password dua kali, pertama di textbox **Password** dan kedua di textbox **Password (retype)**. Bagian **Clear the password cache** digunakan agar jika window diminimize maka Cobian akan meminta Anda untuk memasukkan password lagi jika ingin membuka lagi.



Gambar 6.17 Tab Visuals

Tab **Visuals** berguna mengatur atribut yang berkaitan dengan tampilan Cobian:

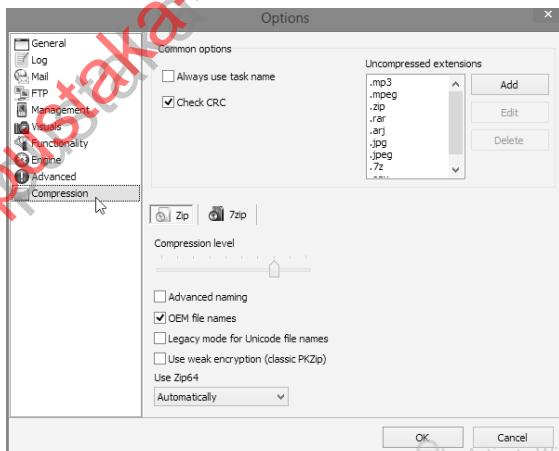
- **Show hints** digunakan untuk memperlihatkan tool tip di interface user.
- **Show icons**, untuk menampilkan ikon.
- **Show number in progress bar** menentukan nomor sebagai angka di progressbar.
- **Show full path** berguna untuk menampilkan semua path dari file yang dibackup.



Gambar 6.18 Tab Functionality

Tab **Functionality** untuk setting yang berkaitan dengan fungsi pokok dari task backup Cobian:

- **Close other instances** untuk menutup instance yang lain.
- **Warn when closing other instance** untuk menampilkan peringatan jika instance lain ditutup.
- **Save special and event settings** membuat setting yang terakhir di Event dan Special akan disimpan oleh program.
- **Calculate sizes** digunakan untuk menghitung ukuran file. Ini bisa memakan waktu dan resource komputer yang cukup lama. Jika komputer Anda tidak terlalu tinggi spesifikasinya, maka hilangkan saja contreng di bagian ini.
- **Show backup hints** berguna untuk menampilkan window petunjuk ketika backup dimulai atau berakhir.
- **Show a dialog box when the backup is done** akan menampilkan dialog box ketika backup sudah selesai.
- **Play a sound when the backup is done** akan menampilkan suara jika backup sudah selesai.
- **Run missed backups** digunakan untuk mengecek apakah ada backup yang belum tereksekusi. Ketika ada, maka user diberi pertanyaan apakah backup akan dilakukan sekarang atau tidak.

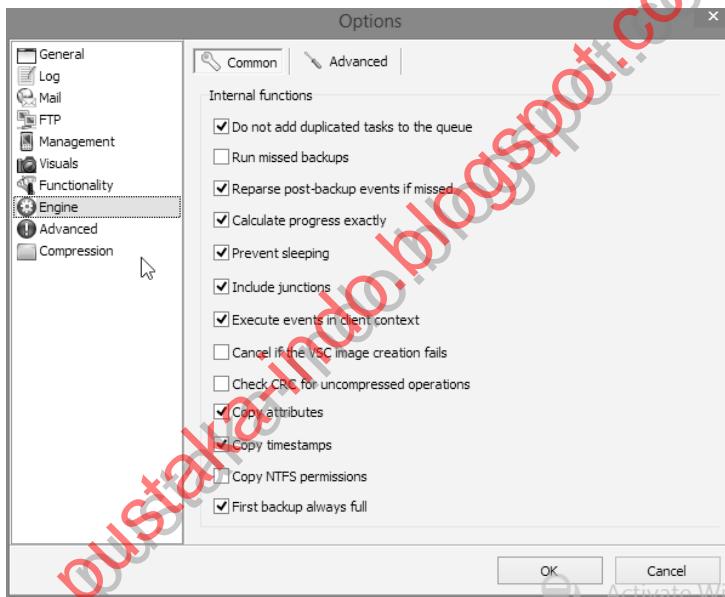


Gambar 6.19 Tab Compression

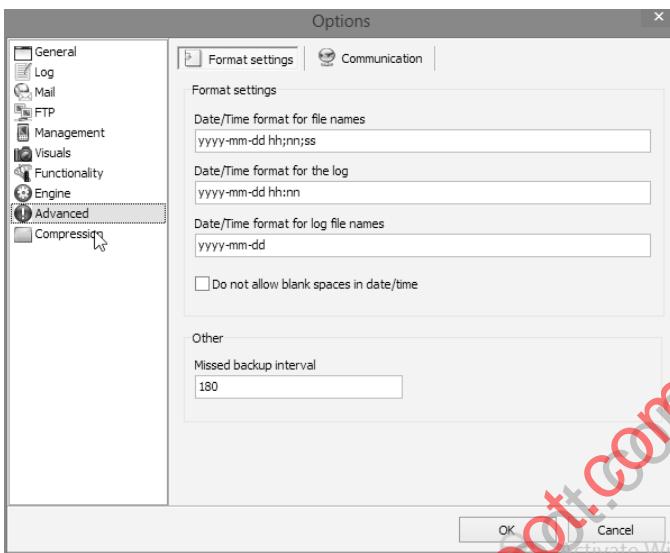
Di tab **Compression**, Anda dapat mengatur bagaimana kompresi yang akan dibuat oleh program Cobian ini:

- Bagian **Check CRC** apabila di contreng akan melakukan pengecekan validitas dari file arsip yang telah dikompresi.
- Bagian **Uncompressed extensions** berguna menentukan ekstensi-ekstensi yang tidak akan dikompresi.
- **Absolute paths** jika dicontreng akan menyimpan lokasi folder di file arsip. Jika tidak, hanya lokasi relatif saja yang disimpan ke file arsip.
- Adapun **OEM file names** akan menjalankan nama file sebagai konversi OEM agar nama file kompatibel dengan ASCII.
- **Advanced naming** akan membuat arsip dipecah-pecah misalnya Archive\_001.zip, Archive\_002.zip, dan seterusnya. Jika tidak dicontreng, maka namanya akan menggunakan nama klasik seperti Archive.zip, Archive.z01, dan seterusnya. Tapi perhatikan bahwa beberapa program zip bisa tidak kompatibel dengan penamaan non klasik.
- Combobox **Use Zip64** akan memilih tipe file zip yang diciptakan. Jika Anda tidak mengaktifkan Zip64, maka file zip yang dihasilkan tidak bisa lebih besar dari 2 Gb. Jika Anda memilih **Automatically**, maka Cobian Backup akan memilihkan metode terbaik untuk tiap file arsip.
- **Zip level** merupakan level pengompresian yang digunakan. Jika Anda memilih 0 maka file tidak akan dikompresi dan hanya disimpan saja di arsip. Sementara, jika Anda memilih 9, maka file akan disimpan ke dalam bentuk kompresi maksimal.
- **Dictionary** menentukan kualitas kompresi. Semakin besar dictionary akan semakin bagus kompresinya. Terutama ketika mengompresi file besar. **Compression level** menentukan level kompresi yang digunakan dengan arsip SQX.
- Bagian **Recovery data** berguna untuk menambah jumlah persen file yang merupakan data yang diperlukan untuk recovery jika file arsip yang dibuat rusak atau tidak sempurna. Nilainya bisa 1 sampai 5. Satuannya persen.

- **Multimedia compression** menerapkan beberapa algoritma kompresi otomatis untuk file-file multimedia, seperti file gambar, suara, dan video. Ini bisa meningkatkan kualitas kompresi. Opsi ini harus diaktifkan jika Anda ingin ukuran file kompresi yang sangat minimal.
- **Exe compression** membuat Cobian akan menerapkan kompresi lossless yang memungkinkan tidak ada kehilangan data ketika mengkomprimasi file executable. File-file yang cocok dengan Exe compression adalah file .Exe, Dll, Driver, dan sebagainya.
- Bagian **Solid archives** dicentang jika Anda ingin membuat file hasil kompresi memiliki ukuran sekecil mungkin.



*Gambar 6.20 Tab Engines di Cobian*



Gambar 6.21 Tab Advanced di pengaturan opsi Cobian

Di tab **Engines** dan **Advanced** ada beberapa opsi yang penting yang berkaitan dangan kegiatan inti backup dan opsi lanjutan:

- **Calculate the progress exactly** menyebabkan engine dari Cobian akan menghitung jumlah file yang akan di-backup sebelum backup dilakukan. Ini agar Anda bisa menghitung persentase total backup sebelum backup dilakukan. Jika checkbox ini tidak dicek maka persentase operasi tidak akan diperlihatkan.
- **Low priority copying thread** dipilih jika Anda merasa tidak terlalu mementingkan kecepatan backup. Backup akan dijalankan lebih lama, namun komputer bisa digunakan untuk kepentingan lainnya karena proses backup sedikit memakan memory.
- **Use several methods for copy** memungkinkan Cobian Backup menggunakan stream untuk meng-copy file.
- **Use only shell methods** akan menggunakan operasi ShFileOperationW untuk menyalin file. Jika Anda ingin atribut file juga disalin, Anda bisa memilih **Copy file attributes**.

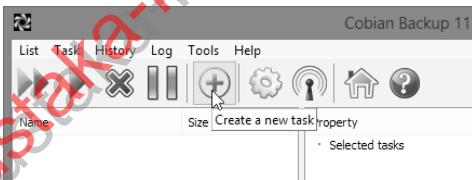
- **Copy the file stamp** akan menyalin filestamp dari file yang di-copy ke file tujuan.
- **Always create directory** akan membuat direktori untuk menyimpan file dengan nama yang sama seperti nama file tersebut.
- **Apply masks to subdirectories** akan menerapkan masking pada subdirektori. Misalnya mask c:\mydir\\*.txt, maka file c:\mydir\subdir\atext.txt akan cocok dengan masking karena mask tersebut cocok, dimana tanda \* merupakan karakter yang mengacu pada semua ekstensi yang ditentukan.
- **Do not separate the timestamp** akan membuat nama file dan timestamp dipisahkan dengan karakter " " dan bukan dengan spasi saja. Misalnya, hasilnya seperti archive-2004-03-21.doc dan bukan archive 2004 03 21.doc.
- **Delete empty directories** untuk menghilangkan direktori kosong dalam tujuan backup.
- **IPC sleep time** menentukan waktu yang digunakan oleh thread IPC untuk sleep. Anda disarankan jangan mengubah opsi ini.
- **Connection timeout** menjelaskan timeout untuk koneksi dalam satuan milidetik untuk protokol TCP/IP.
- **Threads sleep time** menentukan waktu dalam milidetik yang digunakan oleh thread lain untuk sleep. Anda disarankan tidak mengubah opsi ini.
- **Date/time format** menjelaskan pemformatan tanggal dan waktu. Berikut ini simbol format tanggal dan waktu yang bisa Anda gunakan:
  - **d** menampilkan hari sebagai angka tanpa awalan angka 0, jadi angkanya antara 1 sampai 31.
  - **dd** menampilkan hari sebagai angka dengan awalan 0 untuk angka yang 1 digit. Misalnya, 01 sampai 31.
  - **ddd** menampilkan hari sebagai singkatan, nilainya antara Sun sampai Sat.

- **ddd** menampilkan hari sebagai nama penuh, dari mulai Sunday sampai Saturday.
- **m** menampilkan bulan sebagai angka tanpa awalan 0 di depannya, jadi antara 1 sampai 12.
- **mm** menampilkan bulan sebagai angka dengan awalan 0, jadi antara 01 sampai 12.
- **mmm** menampilkan bulan sebagai singkatan, jadi hasilnya adalah dari Jan sampai Dec.
- **mmmm** menampilkan bulan sebagai nama penuh, jadi hasilnya January sampai December.
- **yy** menampilkan tahun sebagai angka 2 digit, antara 00 sampai 99.
- **yyy** menampilkan tahun sebagai angka 4 digit, antara 0000 sampai 9999.
- **h** menampilkan jam tanpa awalan 0, antara 0 sampai 23.
- **hh** menampilkan jam dengan awalan 0, antara 00 sampai 23.
- **n** menampilkan menit tanpa awalan 0, jadi antara 0 sampai 59.
- **nn** menampilkan menit dengan awalan 0, antara 00 sampai 59.
- **s** menampilkan detik tanpa awalan 0, antara 0 sampai 59.
- **ss** menampilkan detik dengan awalan 0, antara 00 sampai 59.
- **z** menampilkan milidetik tanpa awalan 0, antara 0 sampai 999.
- **zzz** menampilkan milidetik dengan awalan 0, antara 000 sampai 999.
- **am/pm** menggunakan 12 jam AM atau PM sebagai awalan dari h atau hh.

- **a/p** sama seperti **am/pm**, hanya saja tulisannya a atau p.
- **Buffer size** menentukan buffer yang digunakan untuk menyalin file.
- Sementara **make the first backup full** akan membuat backup dari file pertama akan penuh.
- **Check CRC for copy operations** akan membuat Anda dapat mengecek CRC dari semua file ketika backup tidak dikompres. Backup menggunakan Check CRC ini umumnya akan lebih lama 3 kali dibandingkan backup tanpa CRC.
- **Copy NTFS permissions** berguna untuk menyalin permission dari NTFS di file. Ini memerlukan hak administrator.
- **Timeout for the UI response** akan menentukan waktu timeout untuk operasi user interface dalam milidetik.

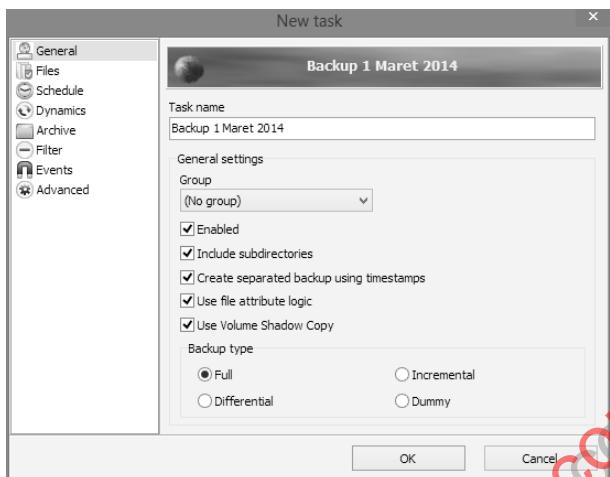
### 6.2.3 Pembuatan Task Backup

Tasks merupakan tool yang membuat Anda dapat menjadwalkan backup pada saat-saat tertentu. Task dapat diciptakan atau dimodifikasi menggunakan button Task di toolbar.



Gambar 6.22 Button untuk membuat task baru

Klik button **Create a new task** untuk membuat task backup baru. Muncul halaman **Properties for: nama\_backup**. Isikan nama task di textbox **Taskname** di tab General seperti gambar berikut.



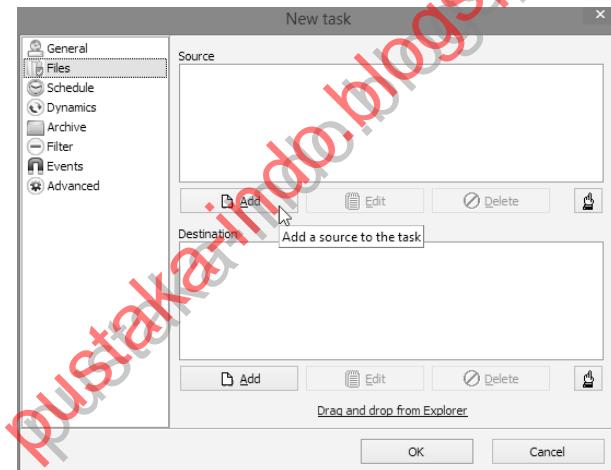
Gambar 6.23 Tab General

Task ID menjelaskan nomor unik yang merupakan identitas dari task. Anda tidak bisa menggantinya karena sudah dibuat secara otomatis oleh program.

- **Disabled** digunakan untuk tidak mengaktifkan task, sehingga task akan tidak diproses ketika dieksekusi, Anda tidak perlu memilih Disabled ini.
- **Include subdirectories** menentukan bahwa folder yang terpilih akan disalin semua sub direktori di dalamnya dan bukan hanya yang di direktori itu saja. **Create separated backups** akan membuat file baru atau direktori baru tiap mem-backup sebuah file atau direktori. Tanggal dan waktu yang digunakan akan dimasukkan ke dalam nama file.
- **Clear the archive attribute** akan membersihkan atribut bit dari file yang menentukan apakah file akan disalin atau tidak dalam backup ketika backup tersebut adalah diferensial atau inkremental.
- **Use file attribute logic** berguna jika Anda mem-backup dari sistem file di Linux, karena di Linux pengaturan kewenangan berjalan sangat longgar.

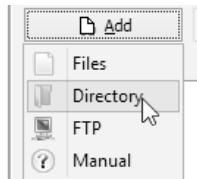
Di backup type ada 4 jenis task backup, penjelasannya seperti berikut:

- **Full backups:** Tiap file di sumber backup akan disalin atau dikompresi. Jika sebelumnya sudah ada file di tempat sebelumnya, maka akan ditimpak. Jika tidak dipilih, maka file sebelumnya akan tetap ada di tempat tujuan backup.
- **Incremental:** Cobian akan menyalin sumber file yang hendak dibackup jika sudah berubah dari backup terakhir kali. Jika tidak ada, maka tidak perlu menyalin file dan file akan diluncurkan untuk menghemat waktu mem-backup.
- **Differential:** Cobian akan mengecek apakah sumber yang hendak dibackup sudah berubah dari terakhir kali backup atau belum dari backup jenis FULL yang terakhir, jika sudah, maka tidak perlu dilakukan backup.
- **Dummy task:** Backup ini tidak perlu menentukan sumber backup dan lokasi tujuan backup. Ini hanya digunakan sebagai waktu penjadwalan untuk mengeksekusi aplikasi, mematikan service, reboot komputer, dan sebagainya.



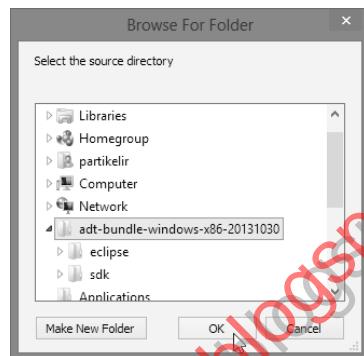
*Gambar 6.24 Tampilan awal tab Files*

Kemudian klik tab **Files**, di sini ada 2 textbox, yaitu **Source** yang digunakan untuk menentukan file atau direktori yang ingin di-backup, dan yang kedua **Destination** yang hendak menentukan tujuan backup. Di button **Add**, Anda dapat menentukan jenis backup, yaitu file, direktori, situs FTP atau menentukan secara manual.



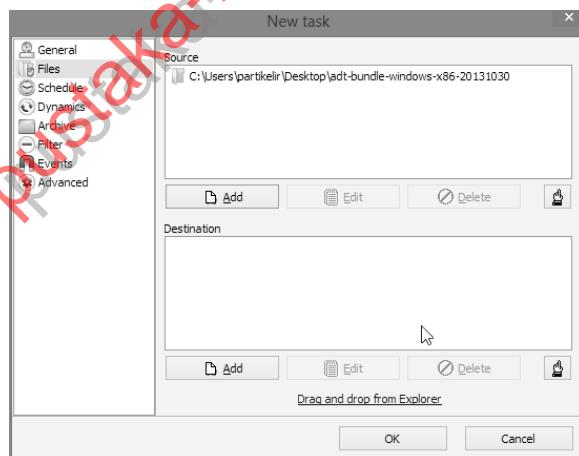
Gambar 6.25 Menentukan jenis yang hendak ditambahkan

Jika memilih directory, maka muncul window **Browser for Folder** yang dapat digunakan untuk memilih folder yang akan di-backup.



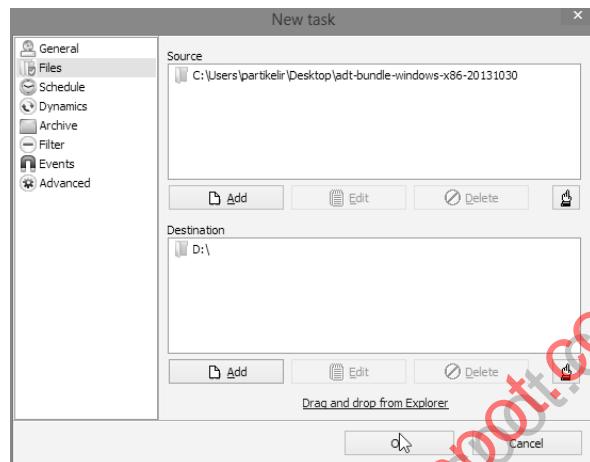
Gambar 6.26 Pemilihan folder yang akan dibackup

Maka, tampilan folder yang akan di-backup terlihat di textbox **Source**, seperti terlihat di gambar berikut.



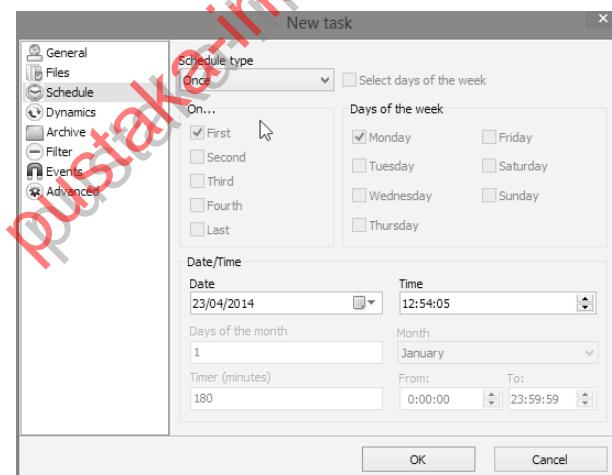
Gambar 6.27 Source folder yang hendak di-backup

Begitu pula pilih folder untuk menampung hasil backup di **Destination**. Anda juga bisa memilih FTP. Khusus FTP, pengisian harus lengkap, jika tidak maka backup akan gagal.



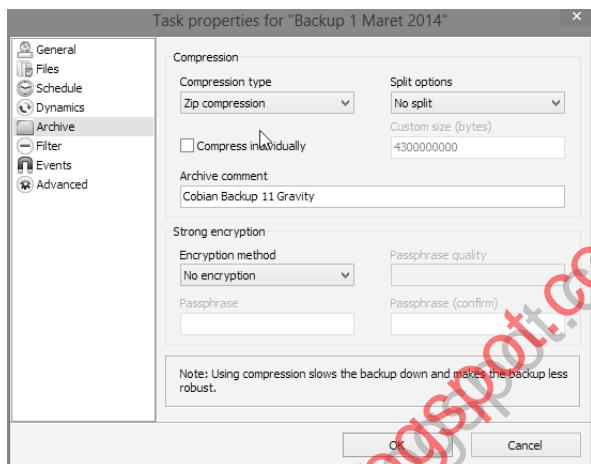
Gambar 6.28 Pemilihan sumber dan tujuan backup

Klik tab **Schedule** untuk menentukan bagaimana task itu dijadwalkan. Anda bisa menentukan eksekusinya sekali saja (once), tiap hari (daily), mingguan (weekly), berdasarkan timer, atau manual.

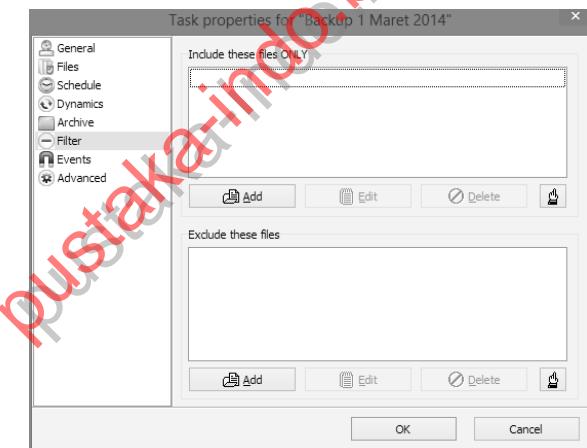


Gambar 6.29 Tab schedule

Tab **Archive** digunakan untuk menentukan file arsip yang akan dibuat. Anda bisa menentukan apakah tidak menggunakan pengarsipan, arsip zip, atau sqx. Anda juga dapat menentukan apakah file kompresi dipotong-potong menjadi beberapa bagian atau tidak?



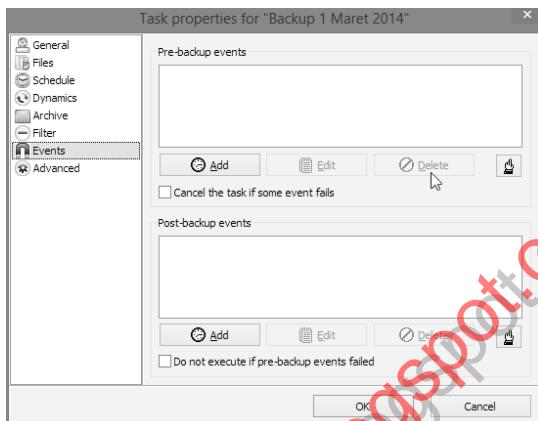
Gambar 6.30 Tab Archive



Gambar 6.31 Tab Special

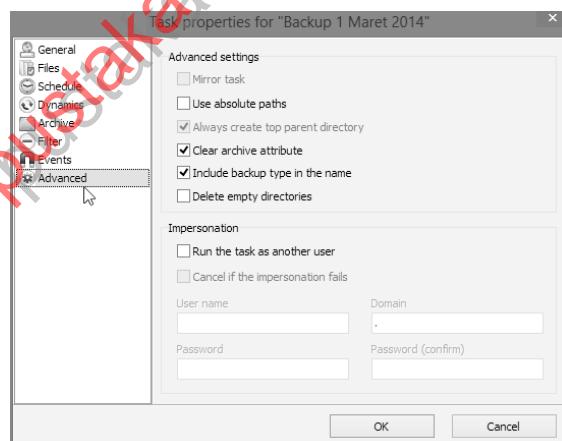
Di tab **Special**, Anda dapat menambahkan daftar file atau direktori yang bisa dikecualikan dari backup. Anda dapat menggunakan beberapa metode:

- **Files:** Hanya dengan memilih menu Add file.
- **Directories:** Memilih direktori dengan mengklik menu Add directory.
- **Enter a mask:** Anda tinggal memasukkan masking, seperti \*.txt untuk mengecualikan file text, dan seterusnya.



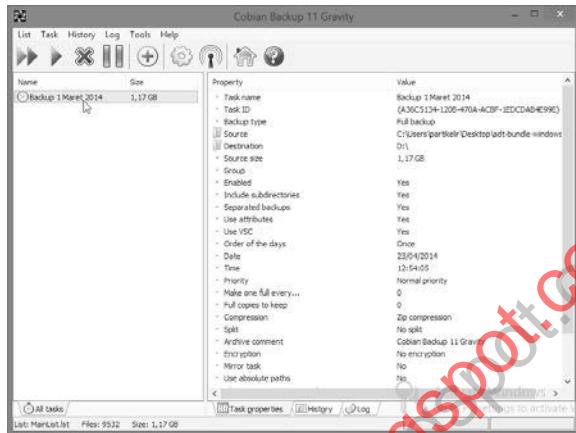
*Gambar 6.32 Tab Events*

Tab **Events** menentukan apa event yang akan dieksekusi sebelum atau setelah backup. Tab **Advanced** bisa digunakan untuk menentukan apakah Anda menjalankan program backup ini sebagai user lain yang tercatat di komputer.



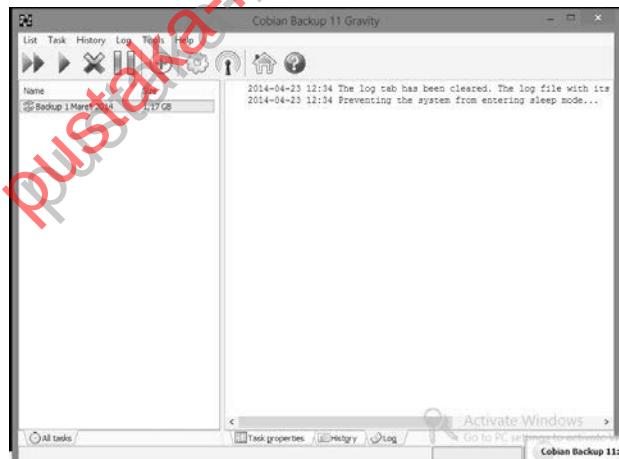
*Gambar 6.33 Tab Advanced*

**Run the task as another user** dipilih jika Anda memerlukan task yang memerlukan akses file dari user lain yang permission-nya tidak Anda miliki. **Abort if failed** menentukan bahwa jika login ke user lain tersebut gagal, maka hentikan pengeksekusian task dan jangan melanjutkan lagi.



Gambar 6.34 Hasil pembuatan task

Setelah dibuat, daftar task akan terlihat di window awal dari Cobian 8 seperti berikut. Untuk mengeksekusinya, klik tombol **Panah** (run task), maka task backup tersebut akan dijalankan hingga selesai dan file backup disimpan di folder yang dituju.



Gambar 6.35 Backup sudah selesai

## BAB

# 7

# Pengamanan Menggunakan Password

Sebuah password merupakan kunci yang digunakan untuk membuka dan mengakses informasi yang umumnya bersifat rahasia dan tersimpan di komputer atau media penyimpanan online. Contohnya, jika Anda memakai email pasti menggunakan password untuk mengakses tool yang harus Anda gunakan.

Walaupun bisa jadi Windows Anda tidak ber-password, namun jika informasi di dalam komputer Anda berharga dan demi alasan keamanan, maka lebih baik Anda mem-password komputer Anda.

## 7.1 Peranan Password

Password adalah tool yang penting dan sifatnya harus sangat rahasia. Namun saat ini, kesadaran pengguna komputer untuk melindungi datanya dengan menggunakan password sangat rendah. Seandainya di-password, mereka masih menggunakan password yang kurang aman.

Kecenderungannya, pengguna komputer masih membuat password menggunakan format yang mudah diingat, misalnya menggunakan nama depan, nama belakang, tanggal lahir, tahun lahir, nomor telepon, nama anak, dan identitas pribadi lainnya.

Beberapa orang lainnya juga masih mencatat password-nya di tempat yang kurang aman. Misalnya di kertas, di file teks, atau file dokumen word. Walaupun ini memudahkan Anda dalam mengingat, namun jika file tersebut bisa terbaca orang, maka bisa membahayakan.

Jika informasi yang Anda simpan sangat rahasia, kemungkinan besar orang yang menginginkannya pun sangat banyak. Apalagi jika disimpan di internet, maka banyak hacker yang berpotensi mengganggu, baik yang sengaja mengincar data Anda, atau pun yang cuma iseng bisa melihat data Anda.

Untuk mengurangi potensi kerusakan dari penggunaan password yang tidak aman, solusinya adalah dengan membuat password yang aman. Bagaimana sebenarnya ciri password yang aman?

Pertama adalah harus cukup panjang. Semakin panjang jumlah karakter password akan semakin bagus kualitas password tersebut. Selain itu, password sukar untuk ditebak jika panjang.

Password yang kuat juga sebisa mungkin mengombinasikan beberapa karakter, yaitu huruf, angka, dan simbol. Tapi ketika menggunakan kata tertentu, pastikan kata tersebut kira-kira sukar untuk ditebak.

Ubah password secara periodik. Ini untuk mempersulit kemungkinan password ditebak.

Jika memang keamanan data nomor satu, maka Anda dapat membuat password yang acak yang sulit untuk ditebak orang. Apakah harus cara manual? Anda dapat memanfaatkan tool-tool yang membantu Anda untuk membuat password acak yang terkostumisasi khusus untuk Anda.

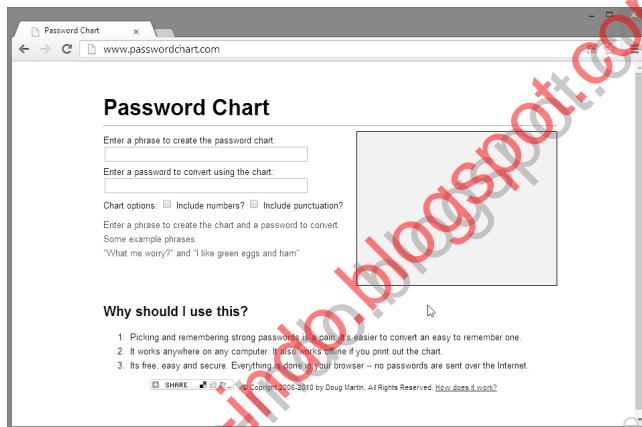
## 7.2 Membuat Password Aman

Ada banyak tool manajemen password yang tersedia di internet. Karena berbasis web, Anda dapat mengaksesnya tanpa harus menginstal sesuatu program di komputer Anda.

Salah satu tool tersebut adalah Password Chart yang membantu Anda membuat password yang kuat berdasarkan 2 parameter yang mudah Anda ingat.

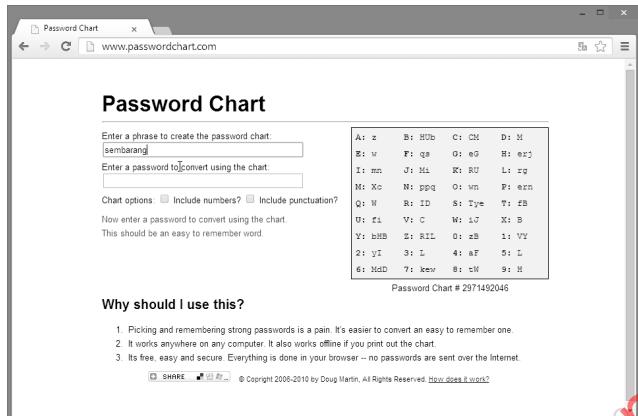
Berikut cara menggunakan password chart:

1. Buka halaman web Password chart di <http://www.passwordchart.com>.
2. Ada 2 textbox di bagian atas, yaitu **Enter a phrase to create the password chart**, Anda bebas mengisikan kata-kata apa pun di sini. Yang kedua adalah **Enter a password to convert using the chart**, ini untuk mengisi password yang nantinya akan diterjemahkan sesuai dengan chart yang dipilih. Dengan demikian, Anda memiliki 2 tingkat pengamanan, pertama adalah frase untuk chart, dan yang kedua password Anda.



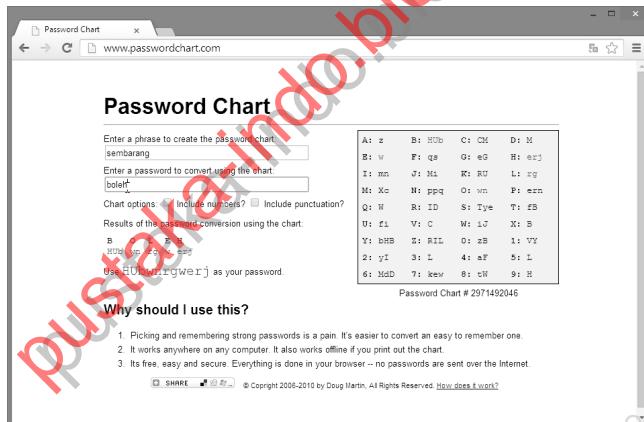
Gambar 7.1 Halaman utama web Password chart

3. Pertama isikan frase untuk membuat chart, setelah Anda mengisikan frase, tampilan chart akan diperlihatkan di bagian **Password Chart**. Karena memakai AJAX, maka perubahan chart di kotak **Password Chart** akan langsung.



*Gambar 7.2 Password chart diisi setelah frase untuk pembuatan chart diisikan*

- Setelah itu masukkan kata untuk password di textbox **Enter a password to convert using the chart.** Kata ini otomatis langsung di parafrasekan menggunakan daftar chart yang dibuat sebelumnya.



*Gambar 7.3 Hasil parafrase*

- Hasilnya terlihat di kalimat **Use [hasil\_password] as your password.** Salinlah hasil password tersebut dan gunakan untuk password Anda. Bagaimana untuk mengingatnya? Mudah saja, Anda tinggal hafalkan kata di textbox **Enter a phrase** dan di textbox **Enter a password**.

### 7.3 Tips Membuat Password

Di bagian 7.1 di atas, sudah sekilas diberitahukan ciri-ciri password yang jelek. Di bagian 7.2 juga telah dijelaskan bagaimana menggunakan tool yang bagus untuk meningkatkan keamanan password. Berikut ini dijelaskan tips dalam membuat password:

- Jangan gunakan informasi pribadi: Jangan gunakan informasi yang berkaitan dengan diri Anda, karena ini akan mudah sekali ditebak. Hacker akan mencoba mencari tahu nama Anda, istri, anak, orang tua, alamat rumah, umur, tahun lahir, dan sebagainya. Hacker juga akan mengombinasikan beberapa data diri tersebut untuk mencoba-coba membuka account Anda.
- Jangan gunakan kata dalam kamus: Salah satu teknik yang dipakai hacker adalah teknik menebak dengan software yang bisa otomatis memadukan kata-kata yang ada di dalam kamus. Jangan kira sulit melakukan ini, komputer sekarang mampu mengenumerasi alternatif ribuan atau bahkan jutaan secara cepat. Karena itu, agar kecil kemungkinan password Anda terdeteksi oleh software yang digunakan oleh hacker, jangan gunakan kata-kata kamus (terutama kata dalam bahasa Inggris).
- Campurbaikan beberapa tipe karakter: Anda bisa membuat password lebih aman dengan mencampurkan huruf besar, huruf kecil, angka, dan karakter seperti '@' atau '%'.
- Gunakan parafrase: Daripada mencoba untuk mengingat password yang diciptakan dengan menggunakan berbagai tipe karakter, lebih baik Anda mencoba untuk membuat kalimat panjang, lalu mengambil huruf-huruf depannya untuk memudahkan Anda mengingat. Misalnya, Anda memiliki hobi memancing, maka Anda bisa memulai dengan kalimat "Aku Suka Memancing Ikan Kakap dan Lele", maka gunakan password "ASMIK&L". Orang pasti akan lebih sulit menduganya.
- Gunakan tool manajemen password: Gunakan tool untuk manajemen password. Tool ini akan menyimpan password dalam jumlah banyak dan kemudian akan mengalokasikan

password jika diinginkan. Ini sebagai pengganti Anda mencatat password di kertas atau file.

- Gunakan password yang berbeda untuk tiap aplikasi: Misalnya, Anda punya password untuk aplikasi Yahoo! Mail, maka gunakan password yang lain untuk aplikasi Google Mail. Ini ibarat pepatah “jangan meletakkan telor dalam satu keranjang”. Jadi jika satu password di-hack, satunya masih aman.
- Jika mampu, ubah password tiap selang waktu tertentu, misalnya sebulan atau dua bulan. Jangan pula gunakan password yang sudah pernah dipakai sebelumnya ketika ingin mengganti.
- Pastikan, Anda tidak melupakan password Anda, walaupun password yang canggih sekalipun dan sulit, tetaplah yang penting adalah aspek manusianya. Jangan sampai Anda membuat password yang sulit ditebak oleh orang lain, tapi juga Anda sendiri malah lupa.

## 7.4 Password Cracker

Ketika menjalankan aksinya, hacker umumnya menggunakan tool password cracker untuk mengetahui password account milik seseorang. Berikut ini beberapa software password cracker yang perlu Anda waspadai:

- **Cain and Abel** bisa download dari <http://www.oxid.it/cain.html>. Ini merupakan tool password recovery yang dijalankan di sistem operasi Windows. Software ini dapat melakukan recovery password dengan melakukan sniffing pada jaringan, meng-crack password yang terekripsi menggunakan berbagai metode seperti Dictionary/kamus, Brute-Force, dan Cryptanalysis attack, merekam chatting VoIP, melakukan decode pada password yang acak, menghidupkan cache dan menganalisis protokol routing. Software ini bisa digolongkan sebagai packet sniffer.
- **John the Ripper** dapat diakses dari <http://www.openwall.com/john>. John the Ripper adalah sebuah tool yang cukup bisa diandalkan untuk mengcrack password. Software ini

dapat dijalankan di beberapa arsitektur komputer yang berbeda, seperti DOS, Windows, BeOS, dan OpenVMS. Software ini mendukung beberapa tipe hash password yang umum terdapat di Unix, seperti Has Kerberos AFS dan Windows LM.

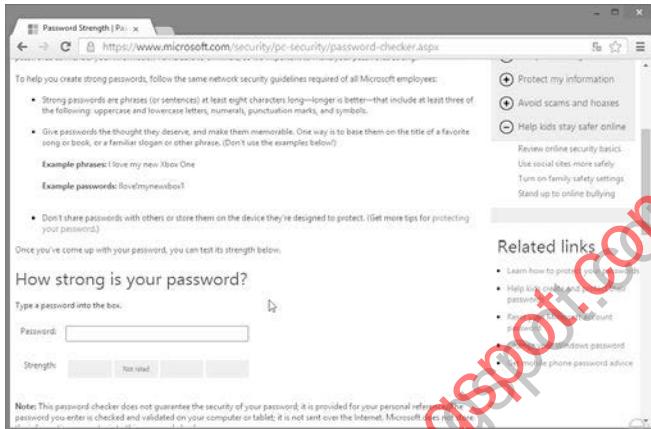
- **THC Hydra** dapat di-download dari <http://www.thc.org/thc-hydra>. Ini merupakan sebuah cracker autentifikasi network. Penggunaan tool THC Hydra ini paling cocok untuk melakukan brute force crack pada layanan yang bersifat remote. Beberapa protokol yang bisa diserang menggunakan THC Hydra antara lain telnet, ftp, http, https, smb, dan sebagainya.
- **Aircrack** dengan situs di <http://www.aircrack-ng.org>. Ini tool crack untuk wireless hacking. Bisa meng-crack WEP/WPA dan 802.11a/b/g. Tool ini mampu menemukan password dengan cukup handal. Software ini juga bisa meng-crack WPA versi 1 dan 2 menggunakan metode kriptografi yang cukup unggul. Aircrack merupakan tool crack yang cukup handal.
- **L0phtcrack**, software ini merupakan software audit dan crack password di Windows. Software ini akan meng-crack berdasarkan hash yang bisa didapatkan dari sebuah komputer dengan sistem operasi Windows. Selain itu, juga bisa dimanfaatkan untuk menyerang server jaringan, PDC (primary domain controller), active directory. Ada banyak metode yang bisa digunakan untuk mendapatkan password, seperti software lainnya, yaitu dictionary dan brute force. Software ini sudah dihentikan pengembangannya oleh Symantec sejak tahun 2006, namun Anda bisa mendapatkan installernya di internet dengan mudah.

## 7.5 Pengecekan Kualitas Password

Seandainya Anda sudah membuat password, maka Anda dapat mengecek kualitas password Anda apakah sudah kuat atau masih belum kuat? Ada beberapa tool pengecek di internet ataupun versi offline yang bisa digunakan untuk mengakomodasi hal ini.

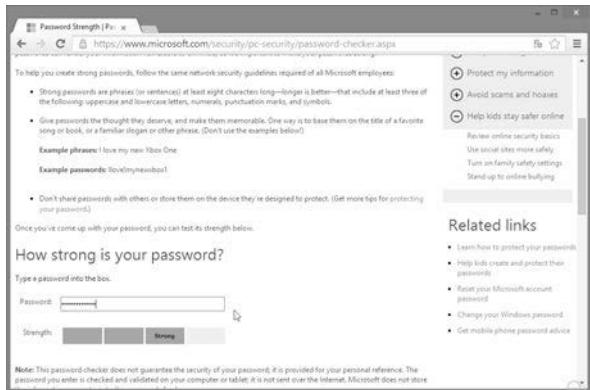
Berikut teknik untuk menguji kualitas password yang disediakan oleh Microsoft:

1. Buka halaman Password checker dari Microsoft.com di alamat <http://www.microsoft.com/security/pc-security/password-checker.aspx>.



Gambar 7.4 Software pengecek password di Microsoft.com

2. Di halaman pengecekan password dari Microsoft.com ada satu textbox **Password** dan di bawahnya ada indikator kualitas password yang digunakan.
3. Isikan password yang telah Anda miliki di textbox **Password** untuk mengujinya.
4. Otomatis, kualitas password tersebut terlihat di bagian **Strength**. Jika password Anda memenuhi syarat password yang baik, maka nilainya **Best** seperti berikut.

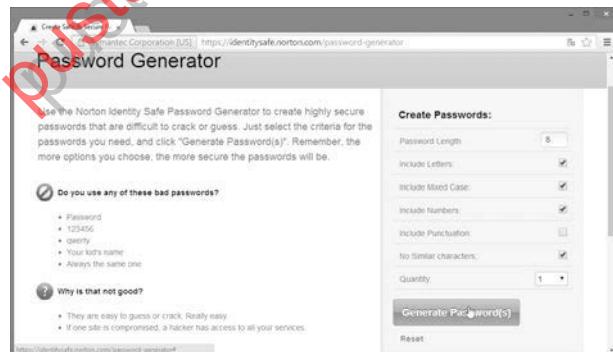


Gambar 7.5 Kualitas password berdasarkan penilaian di Microsoft.com

## 7.6 Password Generator

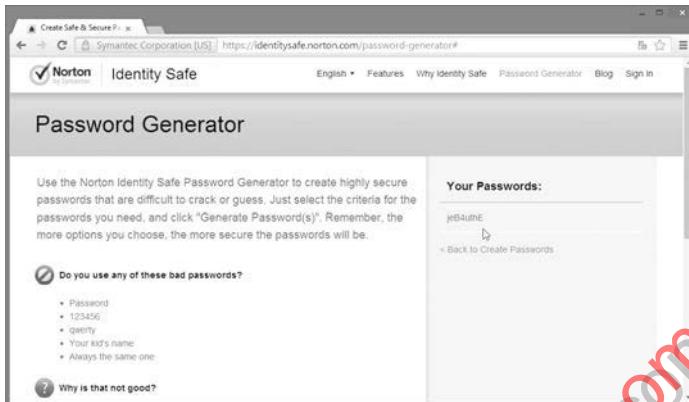
Bingung memilih dan mencari password yang acak dan berkualitas tinggi? Anda bisa memanfaatkan fasilitas password generator yang bisa diakses dengan mudah dari internet ataupun aplikasi desktop. Berikut ini caranya:

1. Buka halaman password generator dari Pctools.com di <https://identitysafe.norton.com/password-generator>.
2. Isikan parameter password yang ingin dibuat di halaman tersebut, misalnya panjang password (password length) dan seterusnya. Klik button **Generate Password(s)** untuk melakukan hal ini.



Gambar 7.6 Halaman untuk generate password di pctools.com

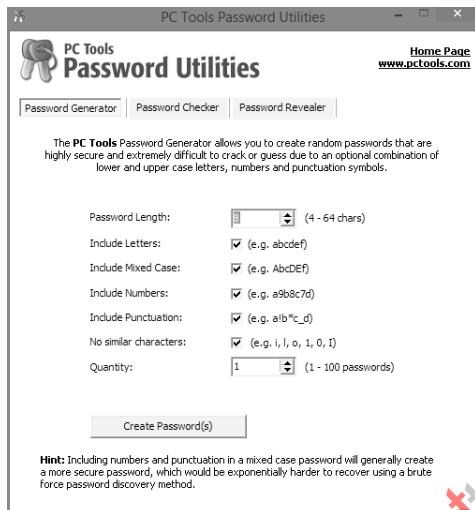
3. Hasilnya dapat Anda lihat di halaman berikutnya.



Gambar 7.7 Hasil pembuatan password

Selain password generator yang online via web, Anda juga bisa men-download software password generator yang berjalan di desktop, sehingga bisa dipakai tanpa terkoneksi ke internet. Berikut ini caranya:

1. Software passutils bisa diperoleh dari <http://www.pctools.com/mirror/passutils.exe>.
2. Eksekusi file tersebut hingga terlihat tampilan berikut. Klik button Yes di bagian PC Tools Password Utilities End user license agreement.
3. Di tab Password Generator Anda dapat memasukkan sifat-sifat password yang hendak dibuat menggunakan tool ini, sama seperti via web. Yaitu panjang password, memasukkan huruf, angka, kuantitas, dan sebagainya. Klik button Create password (s).



Gambar 7.8 Menentukan atribut password yang hendak dibuat menggunakan password generator versi desktop

4. Hasilnya terlihat seperti berikut, di kolom **Passwords** adalah password yang dihasilkan, sementara pengucapan fonetik untuk memudahkan menghafal password adalah di kolom **Phonetic Pronunciation**.

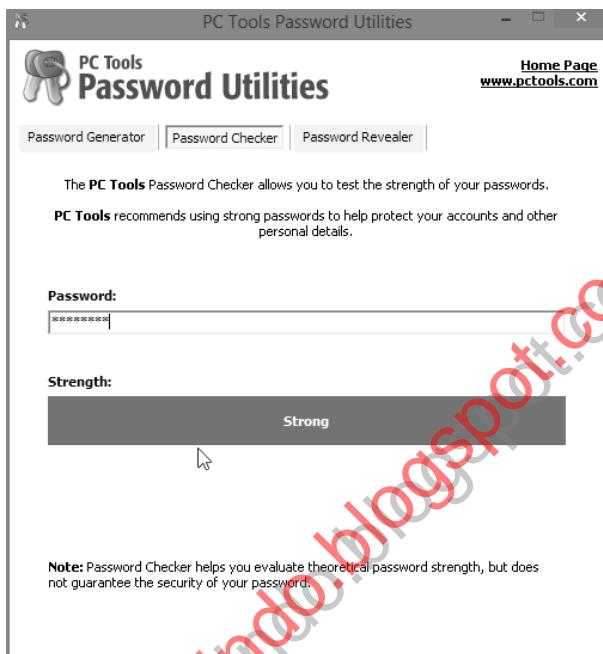
The screenshot shows the same application window as before, but now it displays the results of generating a password. The interface includes a message: 'We have successfully created the password(s) you requested, please remember to store a copy in a safe location as they can not be recreated.' Below this, a table lists the generated password and its phonetic pronunciation:

Passwords	Phonetic Pronunciation
ke3QVb#f	kilo - echo - Three - QUEBEC - VICTOR - bravo - Hash - foxtrot

At the bottom are buttons for '[Copy to clipboard](#)' and '[Save to file](#)'. A red watermark 'Pustaka Informatika.com' is diagonally across the image.

Gambar 7.9 Hasil password yang dibuat

5. Software ini juga sebenarnya punya tool untuk menguji kualitas password yang dihasilkan, yaitu di tab **Password Checker**. Masukkan password Anda dan hasilnya otomatis terlihat di **Strength**.



Gambar 7.10 Hasil pengujian kekuatan password

# BAB

# 8

# Download dan Instalasi Program

Download adalah salah satu jalan masuk software-software jahat ke komputer Anda. Karena itu, salah satu teknik untuk mencegah infiltrasi software-software busuk ke komputer adalah dengan mengerti cara download program yang baik.

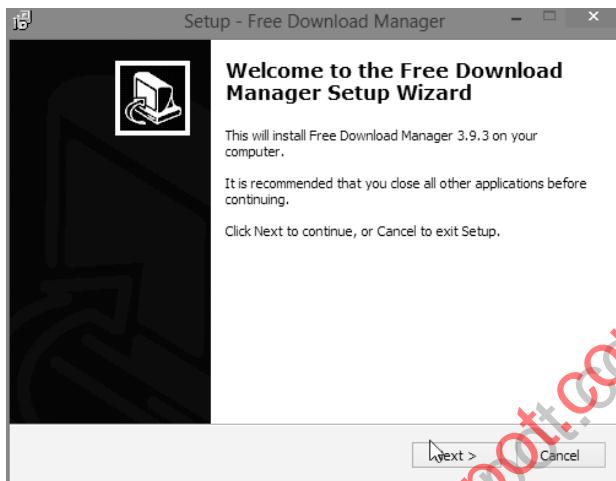
Jika sebuah program busuk secara tak sengaja atau bisa juga disengaja (karena ketidaktahuan) masuk ke komputer, lantas program tersebut diinstall di komputer, maka komputer Anda bisa error terjangkit berbagai macam penyakit. Oleh karena itu, proses download yang aman merupakan sebuah teknik pencegahan/preventif dari penyakit komputer.

## 8.1 Free Download Manager

Salah satu software download terbaik yang tidak hanya oke dari segi kehandalan dalam men-download, namun juga keamanannya adalah Free Download Manager yang bisa di-download dari <http://freedownloadmanager.org>.

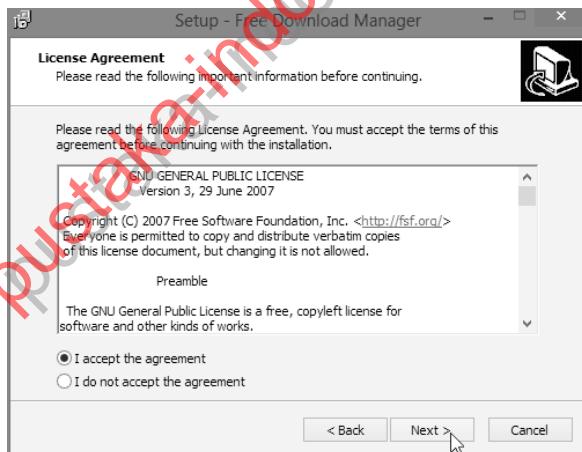
Untuk menggunakan software ini, pertama kali Anda harus menginstalnya terlebih dahulu dengan langkah seperti berikut:

1. Eksekusi file instalasi, di window **Welcome to the Free Dowload Manager Setup Wizard**, klik button **Next**.



*Gambar 8.1 Jendela Welcome to the Free download manager setup wizard*

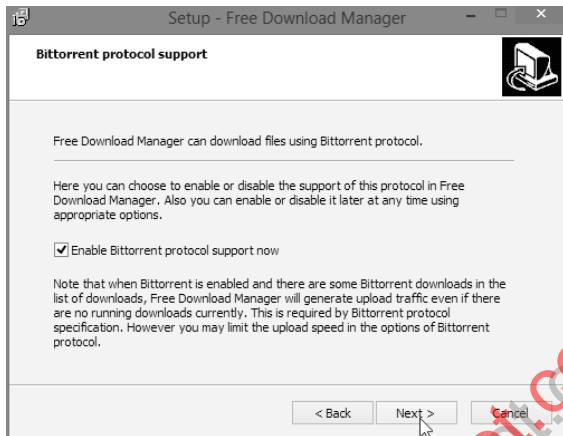
2. Di License agreement, pilih pada radio button I accept the agreement, kemudian klik button **Next**.



*Gambar 8.2 License Agreement*

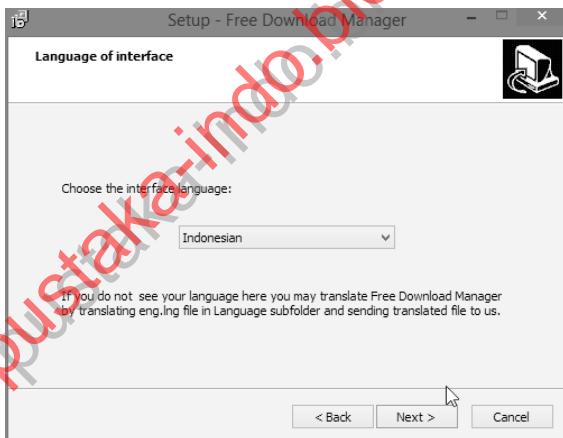
3. Apabila Anda ingin download protokol bittorrent, Anda bisa mengaktifkan **Enable bittorrent protocol support now**.

Namun, Anda bisa mengaktifkannya nanti ketika sudah terinstal. Klik button **Next**.



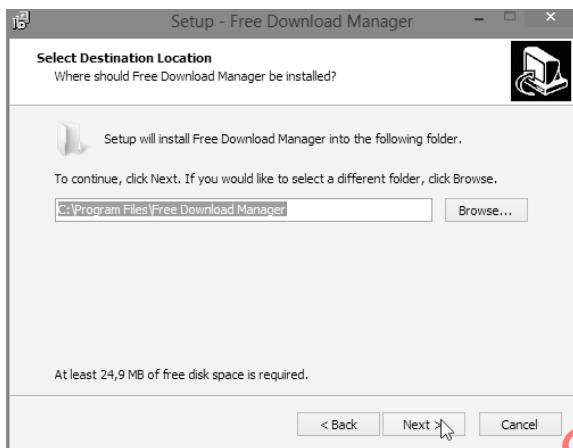
**Gambar 8.3 Protokol Bit Torrent**

4. Pilih bahasa untuk antarmuka program ini di **Choose the interface language**. Klik button **Next**.



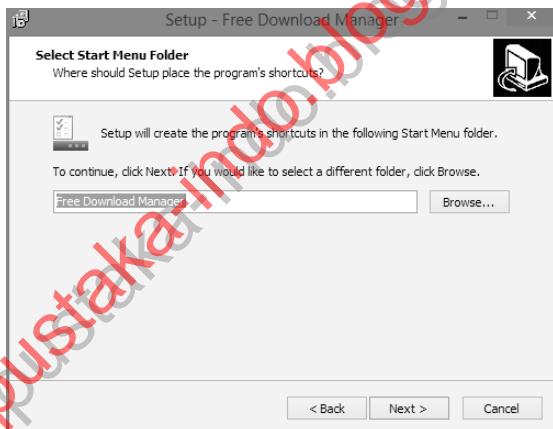
**Gambar 8.4 Pilih bahasa di Choose the Interface language**

5. Berikutnya, pilih lokasi instalasi FDM di harddisk pada window **Select destination location**. Klik **Next**.



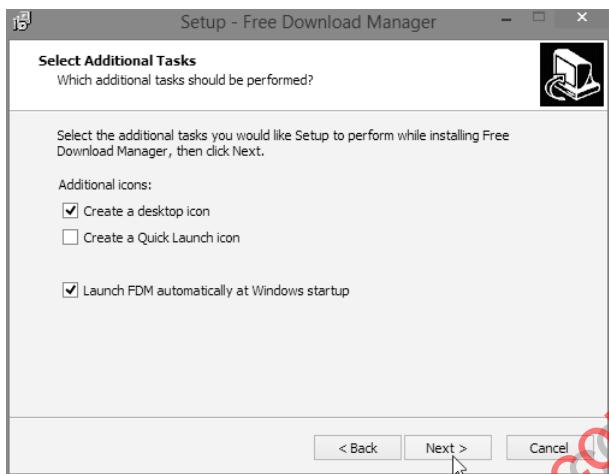
**Gambar 8.5 Pemilihan lokasi instalasi**

6. Isikan nama untuk Start Menu di window **Select Start Menu Folder**. Klik lagi **Next** untuk menuju langkah instalasi selanjutnya.



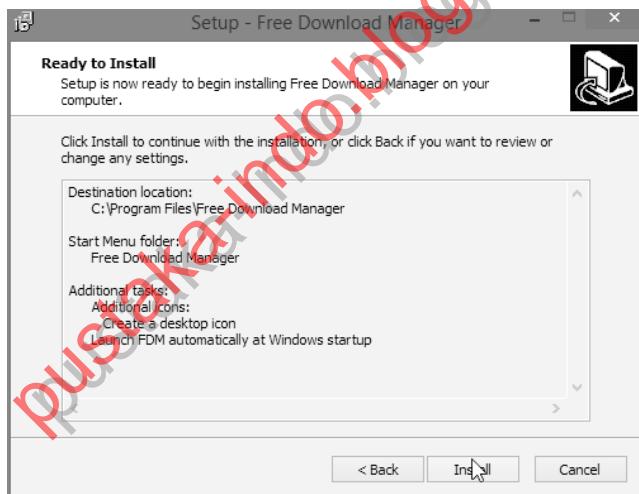
**Gambar 8.6 Penentuan nama di Start Menu**

7. Di **Select Additional Tasks**, Anda dapat menentukan apakah Anda ingin membuat ikon shortcut di Desktop dan Quick Launch. Anda juga bisa menentukan apakah FDM otomatis dieksekusi ketika Windows dimulai. Klik **Next** untuk melanjutkan.



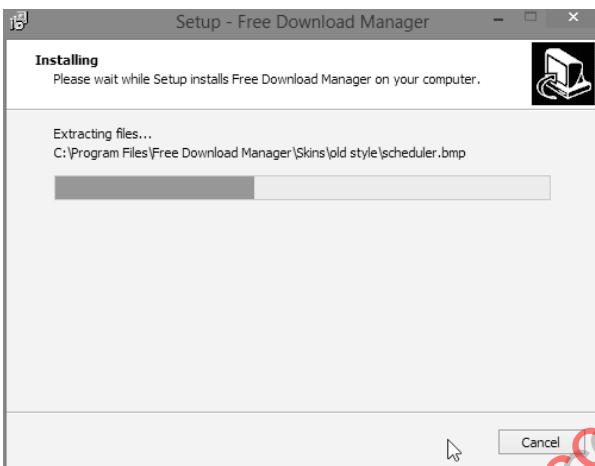
**Gambar 8.7 Pilihan di Additional Tasks**

8. Setelah semua atribut instalasi dipilih, klik **Install** untuk memulai instalasi.



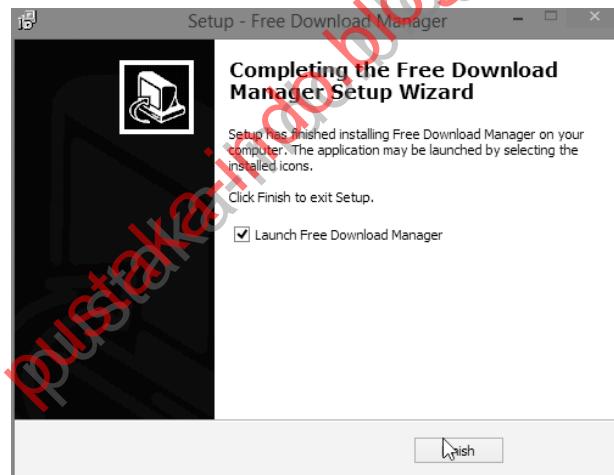
**Gambar 8.8 Instalasi siap dimulai**

9. Tunggu hingga instalasi selesai berlangsung.



*Gambar 8.9 Instalasi berlangsung*

10. Setelah instalasi selesai, klik button **Finish** di window **Completing the FDM Setup Wizard**. FDM pun siap dipakai untuk melakukan safe download di komputer Anda.



*Gambar 8.10 Instalasi FDM sudah komplit*

## 8.2 Download dengan Aman

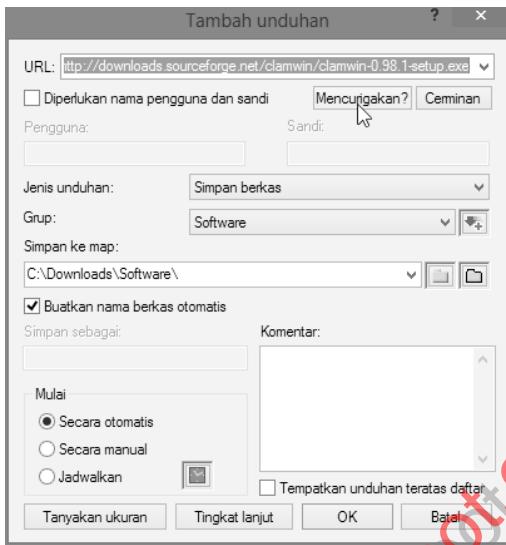
Untuk men-download dengan aman, FDM merupakan salah satu yang menyediakan pengecekan apakah sebuah link mencurigakan atau tidak? Ini adalah berkat fitur komunitas yang ada di FDM. Sehingga, Anda bisa melihat apakah sebuah file di internet aman atau tidak dengan menggunakan fitur ini. Berikut cara untuk mendownload file dengan aman dengan menggunakan FDM:

1. Anda bisa men-download dari sembarang tempat, misalnya dari download.com yang merupakan software uji coba. Anda dapat mengklik link Download dari tempat-tempat download sesuai keinginan Anda.



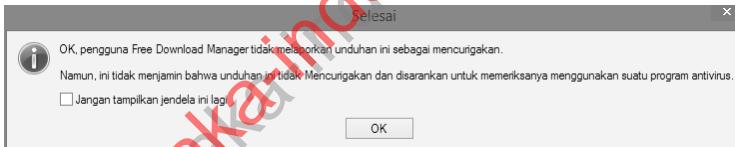
Gambar 8.11 Melakukan download dari salah satu provider Download

2. Kemudian, muncul jendela **Add Download** dengan link URL otomatis terisikan (atau Anda bisa juga mengisikan manual jika sudah memiliki alamat download).
3. Untuk menguji apakah URL dari file yang ingin didownload tersebut adalah malware, Anda dapat mengklik button **Malicious?**



Gambar 8.12 Jendela Add Download

4. Jika tak ada indikasi bahwa file tersebut merugikan, Anda dapat melihat box konfirmasi, OK, Free download manager's users did not report this download as malicious.



Gambar 8.13 Indikasi bahwa tidak ditemukan indikasi bahwa file tersebut adalah file jahat

5. Misalnya, Anda hendak memberikan pendapat, Anda pun langsung bisa melakukannya tanpa harus login atau registrasi terlebih dahulu. Anda tinggal mengklik pada file yang sudah di-download atau tengah di-download, kemudian klik tab Opinions di bagian bawah dari halaman FDM ini.
6. Semua textbox adalah optional, Anda bisa memasukkan pendapat pada textbox Review. Anda juga bisa memberi rate pada file ini. Kemudian klik OK.

Nama berkas	Ukuran	Terunduh	Waktu ...	Pecahan	Kecepatan	Komentar
✓ DS SDQQ2.pdf	156 KB	100% [156 KB]		0/1		
✓ DS SDPS1A.pdf	327 KB	100% [327 KB]		0/1		
✓ SD SDQQ1A.pdf	284 KB	100% [284 KB]		0/1		
✓ DS SD2.pdf	407 KB	100% [407 KB]		0/1		
<input checked="" type="checkbox"/> DS CTU1.pdf	407 KB	100% [407 KB]		0/1		
✓ DS CTU2.pdf	433 KB	100% [433 KB]		0/1		
✓ SD CTUP1.pdf	188 KB	100% [188 KB]		0/1		
✓ DS CTUP2.pdf	625 KB	100% [625 KB]		0/1		

Pencatat | Laju | Penampilan/konversi Media | Pendapat

Please share your opinion on this file with community!

\* Url:

\* File title:

\* Your name:  \* Your email:

Review title:

\* Review:

View other community members opinions on this download.

\* Rate this file:   Warn about malicious download

**Gambar 8.14 Pemberian opini mengenai URL dari download tertentu di FDM**

7. Tanda bahwa komentar Anda sudah masuk di server FDM adalah ada tulisan **Thank you a lot for helping us create an opinion database.**



**Gambar 8.15 Informasi opini Anda tentang sebuah download sudah masuk**

8. Untuk melihat komentar orang lain yang sudah mendownload sebuah software, Anda juga bisa mengklik link **View other community members opinions on this download.**

■ Url:

■ File title:

■ Your name:  ■ Your email:

■ Review title:

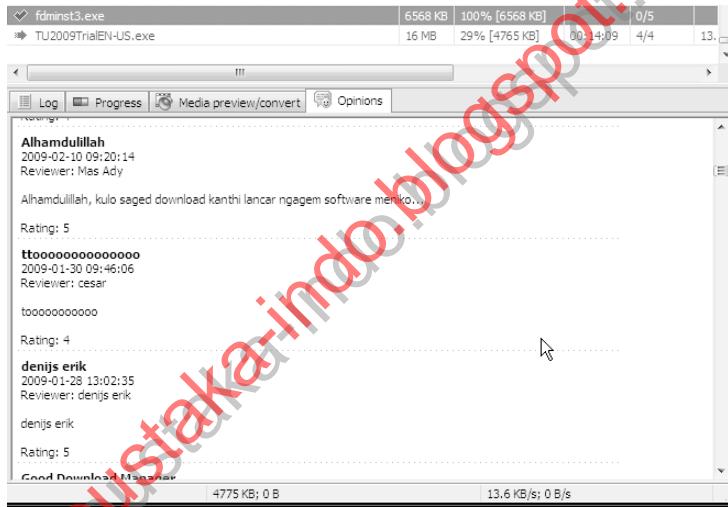
■ Review:

[View other community members' opinions on this download](#)

■ Rate this file:   Warn about malicious download

**Gambar 8.16 Link untuk melihat komentar orang lain tentang sebuah download**

9. Tampilan komentar untuk link download terlihat seperti berikut.



**Gambar 8.17 Tampilan komentar beberapa orang tentang link download**

## BAB

# 9

# Penggunaan Enkripsi

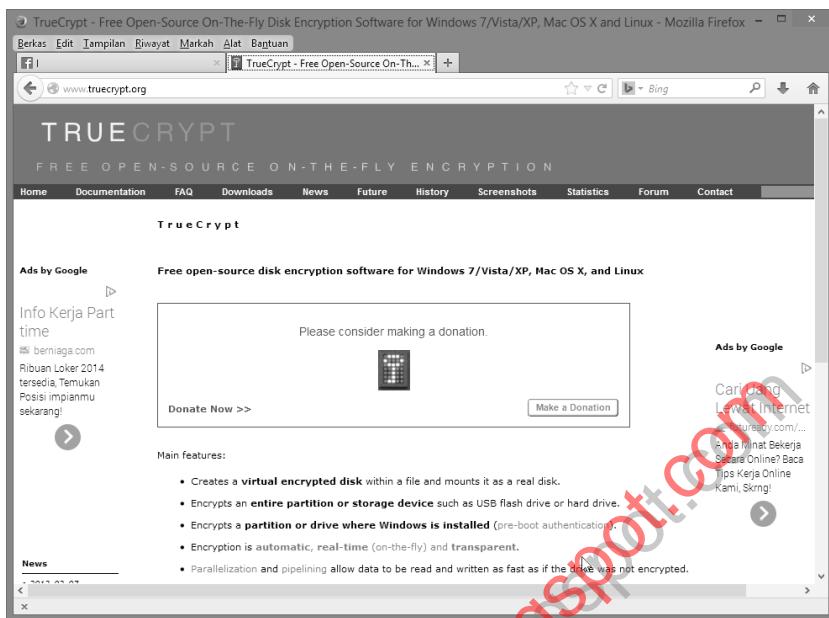
Jika Anda ingin menyimpan sebuah file dan tidak ingin sembarang orang bisa melihat atau mengaksesnya, maka enkripsi lah jalan keluarnya. Enkripsi adalah sebuah teknik untuk melakukan transformasi pada sebuah informasi menggunakan algoritma tertentu, sehingga tidak bisa dilihat oleh orang yang tidak memiliki keahlian untuk mendekripsi informasi tersebut.

## 9.1 Mengenal TrueCrypt

Software yang akan dibahas pada bab ini adalah TrueCrypt, sebuah software open source yang multiplatform dan mendukung banyak teknik enkripsi yang memungkinkan seorang menyimpan rapat informasi di komputernya dengan enkripsi plus dilengkapi dengan pengamanan password.

TrueCrypt merupakan software yang fungsinya melakukan enkripsi volume password secara on the fly. Artinya, data otomatis dienkripsi dan didekripsi menggunakan prinsip *Just In Time* (JIT) yaitu pada saat di-load atau disimpan tanpa harus diatur oleh user.

Dengan demikian, data yang disimpan ke file yang dienkripsi oleh TrueCrypt tidak bisa dilihat oleh sembarang orang karena dienkripsi dan dipassword. Orang harus mengetahui password dan key enkripsi untuk mengaksesnya. TrueCrypt ibaratnya adalah hard disk yang terenkripsi yang bisa *di-mount* menggunakan password. Situs resmi dari TrueCrypt ada di <http://www.truecrypt.org/>.



Gambar 9.1 Halaman download Truecrypt

Namun, begitu volume yang dibuat menggunakan TrueCrypt sudah di-mount maka Anda dapat menganggapnya sebagai sebuah partisi hard disk biasa, dan dapat memperlakukannya seperti drive biasa di Windows Explorer.

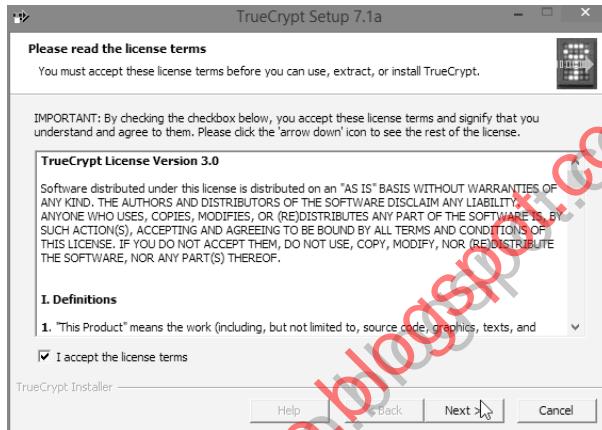
Di antara fitur yang bisa dilakukan oleh TrueCrypt adalah:

- Membuat disk virtual yang terenkripsi dan menyimpannya dalam sebuah file. Ketika file tersebut di-mount, maka ibaratnya seperti hard disk nyata.
- Mengenkripsi partisi atau piranti penyimpanan portabel seperti USB Flash disk.
- Mengenkripsi partisi atau drive di mana Windows diinstal. Ini akan membuat TrueCrypt dijalankan sebelum booting Windows. Dengan demikian, Anda dapat membuat sistem operasi tersembunyi dan file yang tersembunyi.
- Mendukung banyak algoritma enkripsi seperti AES-256, Serpent, dan Twofish. Mode operasinya adalah XTS.

## 9.2 Menginstal TrueCrypt

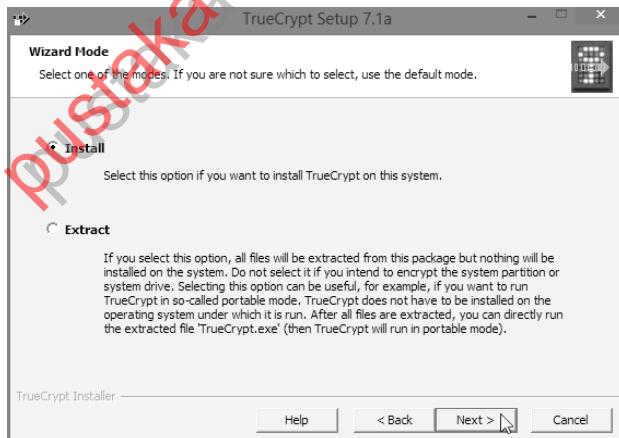
TrueCrypt diinstal di Windows menggunakan prinsip instalasi. Cara berikut merupakan gambaran instalasi/setup dari TrueCrypt:

1. Eksekusi file installer dari TrueCrypt, di window License yang muncul pertama kali, klik button **Accept** setelah sebelumnya mencontreng checkbox **I accept and agree to be bound by the license terms**. Klik button **Accept**.



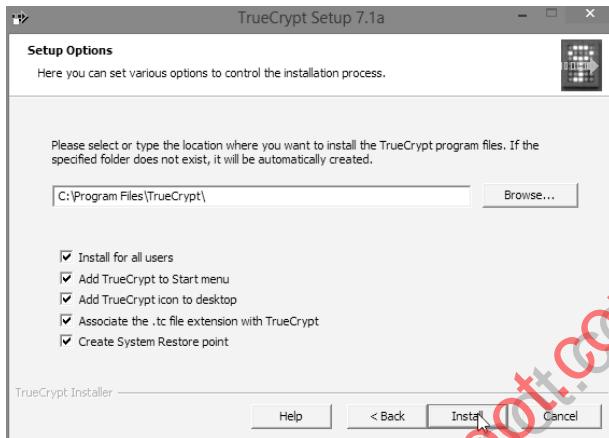
Gambar 9.2 License dari TrueCrypt

2. Di Wizard Mode, pilih radiobutton **Install**. Klik button **Next**.



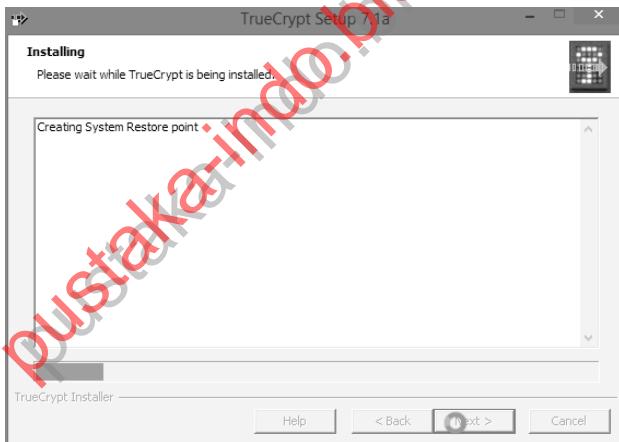
Gambar 9.3 Memilih Install di Wizard Mode

3. Pilih lokasi instalasi TrueCrypt di textbox yang ada di window **Setup Options**. Tentukan juga opsi di checkbox yang ada di bawahnya. Klik button **Install**.



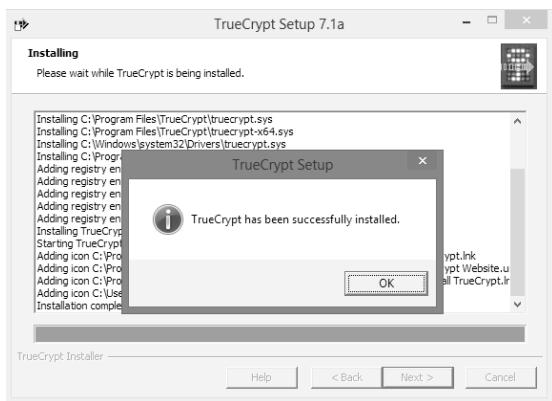
*Gambar 9.4 Pilihan di Setup Options*

4. Tunggu hingga proses instalasi selesai.



*Gambar 9.5 Proses instalasi TrueCrypt sedang berlangsung*

5. Tandanya adalah muncul box dengan tulisan **TrueCrypt has been successfully installed.**

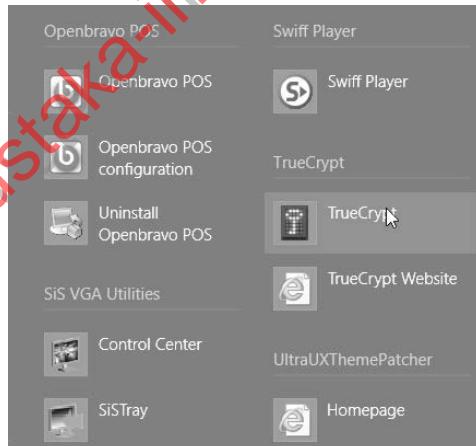


*Gambar 9.6 TrueCrypt has been successfully installed*

### 9.3 Membuat Kontainer Terenkripsi

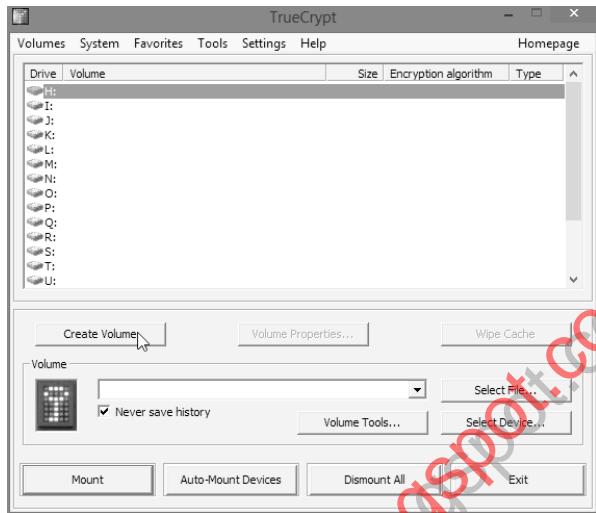
Fungsi utama dari TrueCrypt adalah membuat file yang terenkripsi di mana di dalamnya Anda bisa menyimpan file yang tidak bisa dibuka oleh semua orang atau semua program kecuali oleh TrueCrypt. Itupun harus di-mount terlebih dahulu. Simak langkahnya berikut ini:

1. Akses TrueCrypt dari StartScreen.



*Gambar 9.7 Akses TrueCrypt*

2. Pertama, buat dahulu TrueCrypt container dengan membuka aplikasi TrueCrypt, lalu mengklik button **Create Volume** di window utama TrueCrypt.



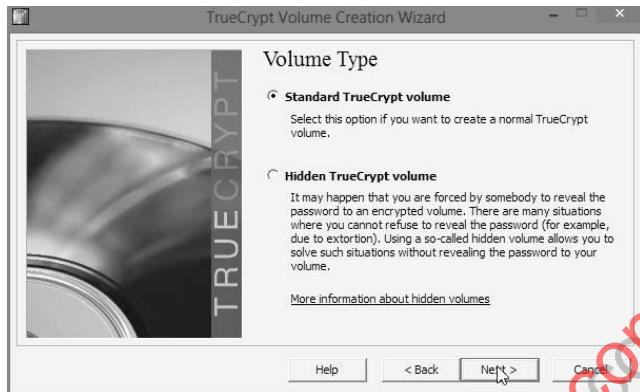
*Gambar 9.8 Klik pada button Create volume untuk membuat volume terenkripsi*

3. Muncul wizard untuk membuat TrueCrypt volume. Di window pertama, pilih **Create an encrypted file container**. Ini akan membuat volume terenkripsi yang bisa dibuka menggunakan TrueCrypt. Klik button **Next**.



*Gambar 9.9 Pemilihan di pemilihan jenis layanan enkripsi yang diinginkan*

4. Di window **Volume Type**, pilih **Standard TrueCrypt volume**. Klik lagi button **Next**.



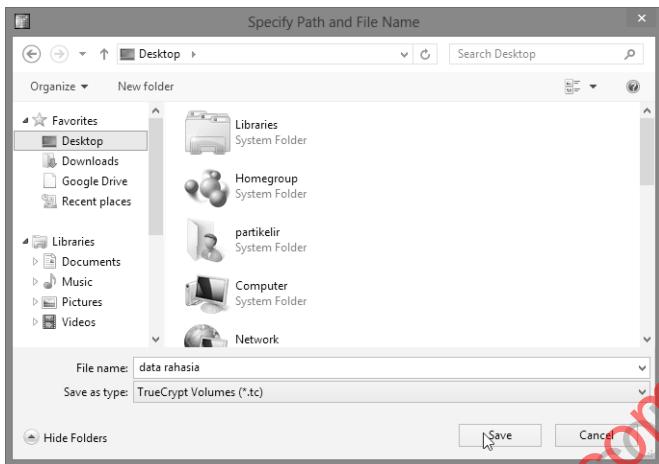
Gambar 9.10 Pemilihan Volume Type

5. Di **Volume Location**, klik button **Select File** untuk menentukan file yang akan menjadi volume terenkripsi. Cek juga pada **Never save history**.



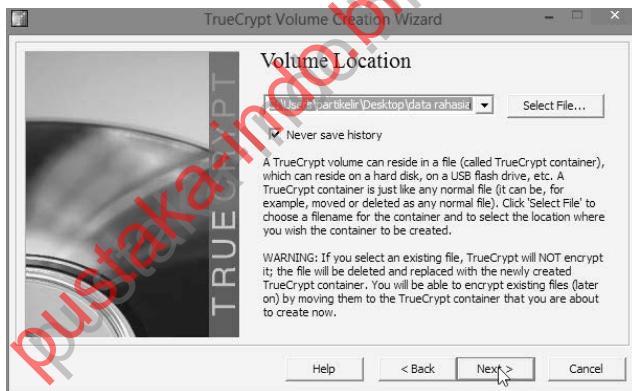
Gambar 9.11 Penentuan Volume Location

6. Muncul window **Specify path and file name**. Isikan nama sembarang di textbox **Filename**, Anda boleh tidak mengisikan ekstensi di textbox **Filename**. Klik button **Save**.



**Gambar 9.12 Penentuan path dan nama file yang akan menjadi volume**

- Setelah kembali ke window Volume Location, Anda bisa melihat lokasi file ditampilkan pada combobox Volume Location. Klik button Next.



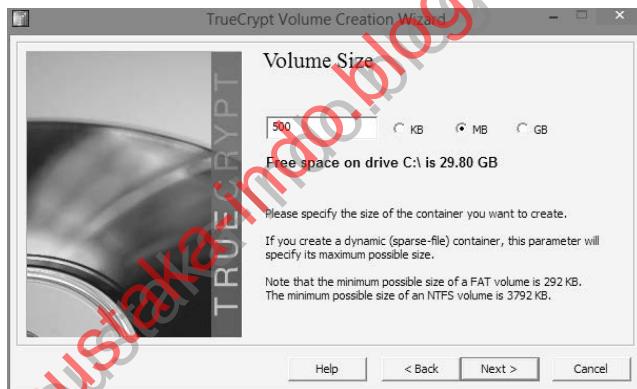
**Gambar 9.13 Pemilihan Volume Location**

- Berikutnya, Anda pilih jenis algoritma enkripsi di groupbox Encryption Algorithm, Anda juga bisa menentukan algoritma hash di groupbox Hash Algorithm. Klik button Next.



Gambar 9.14 Penentuan *Encryption Options*

9. File yang akan menjadi volume terenkripsi perlu diatur kapasitasnya di Volume size. Ukurannya harus lebih kecil dibandingkan kapasitas kosong di partisi harddisk tempat letaknya file tersebut. Klik Next.



Gambar 9.15 Penentuan ukuran file yang menjadi volume terenkripsi

10. Isikan password untuk mengakses volume ini. Isikan dua kali untuk menghindari kesalahan ketik di textbox **Password** dan **Confirm**.



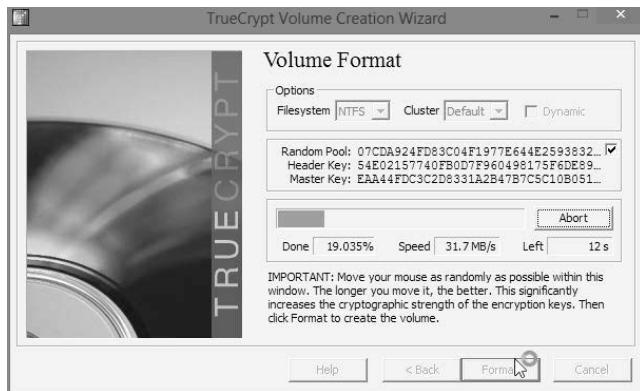
Gambar 9.16 Penentuan password untuk mengakses Volume

11. Tentukan format volume di window **Volume Format**. Yang bisa ditentukan adalah **Filesystem** dan **Cluster** set saja ke **Default**, kemudian klik button **Format** untuk memformat volume tersebut, sehingga volume tersebut ibarat harddisk virtual dengan format sesuai yang dipilih.



Gambar 9.17 Penentuan volume format

12. Ketika proses format berlangsung, terlihat progressbar menunjukkan kemajuan pemrosesan format. Jangan klik button **Abort** karena akan membatalkan proses pemformatan.



Gambar 9.18 Pemformatan volume sedang berlangsung

13. Setelah volume terbuat, Anda dapat mengklik button Exit di window Volume created.

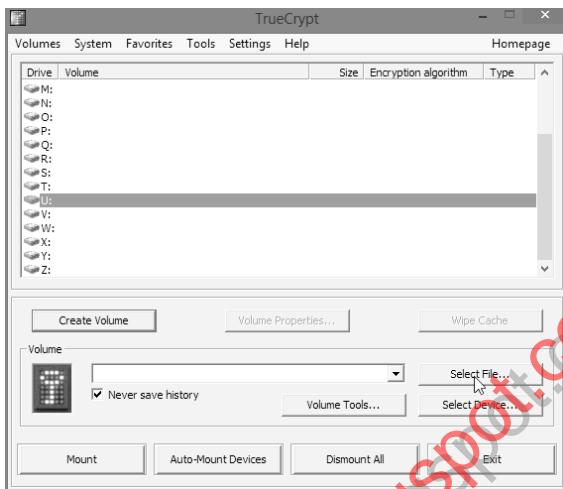


Gambar 9.19 Volume sudah terbuat

## 9.4 Mounting File

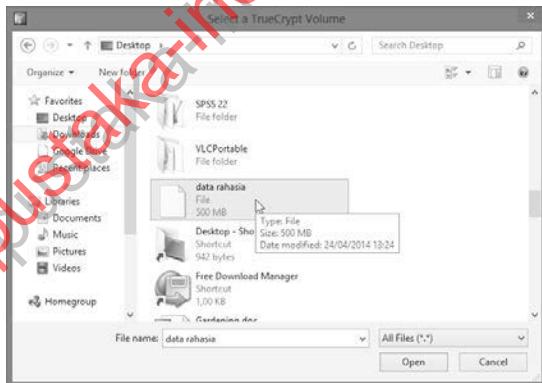
Mounting File adalah kegiatan melakukan mount file volume terenkripsi ke drive tertentu, sehingga volume terenkripsi tersebut berlaku seperti halnya harddisk normal. Berikut ini cara mount file di TrueCrypt:

1. Di window utama TrueCrypt, pilih drive yang hendak menjadi tempat mount, misalnya drive U. Kemudian, klik button **Select file**.



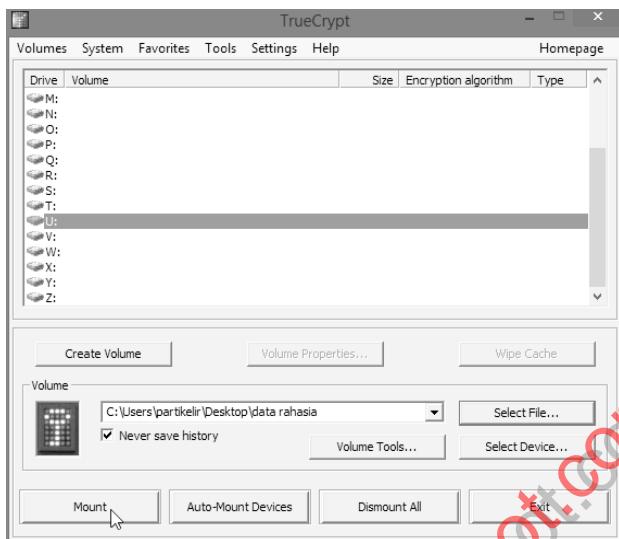
Gambar 9.20 Pemilihan drive dan klik pada button Select file

2. Di window **Select a TrueCrypt volume**, pilih file dari volume terenkripsi yang sudah terbuat sebelumnya. Klik button **Open**.



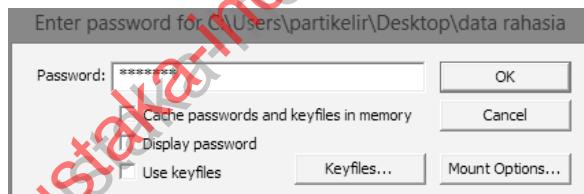
Gambar 9.21 Memilih file volume terenkripsi untuk di-mount

3. Kembali ke window utama TrueCrypt, klik button **Mount** untuk memount drive dengan volume yang sudah terbuat.



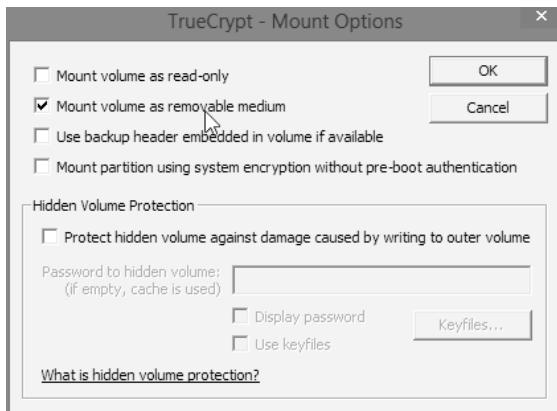
**Gambar 9.22 Button Mount untuk me-mount drive U dengan volume yang sudah terbuat**

4. Masukkan password di textbox **Password** ketika muncul box **Enter password for nama\_volume**. Anda bisa meng-klik button **Mount Options** untuk menentukan opsi tambahan tentang mounting.



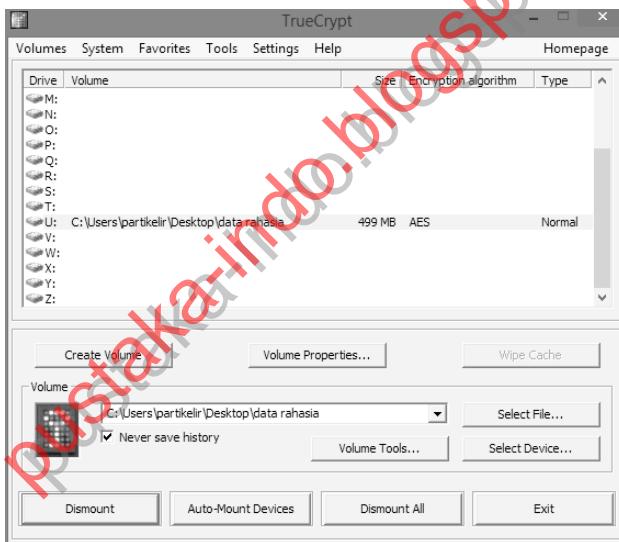
**Gambar 9.23 Memasukkan password untuk mount**

5. Misalnya, Anda ingin menjadikan file volume tersebut seolah removable disk, maka contreng pada **Mount volume as removable medium**. Klik button **OK**.



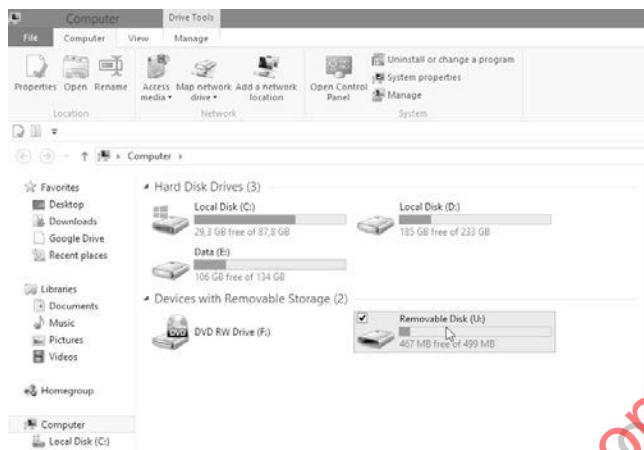
Gambar 9.24 Pilihan di Mount options

6. Maka, terlihat di window utama program TrueCrypt bahwa file volume terenkripsi tersebut sudah ter-mount.



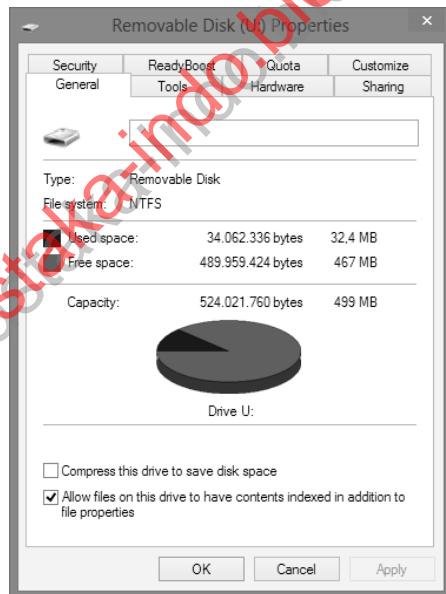
Gambar 9.25 File volume terenkripsi sudah di-mount ke drive U

7. Lihat di Windows Explorer untuk melihat buktinya, yaitu adanya removable disk dengan nama logis **Removable Disk** di drive U.



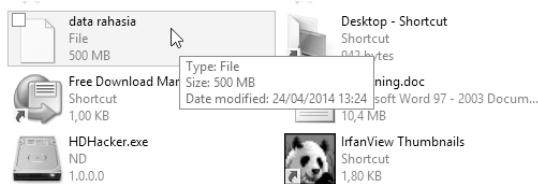
Gambar 9.26 Adanya removable disk dengan nama drive U

8. Jika diklik kanan dan dilihat menu Properties, maka terlihat disk tersebut masih kosong dan dengan kapasitas sesuai dengan kapasitas yang ditentukan ketika volume terenkripsi tersebut dibuat.



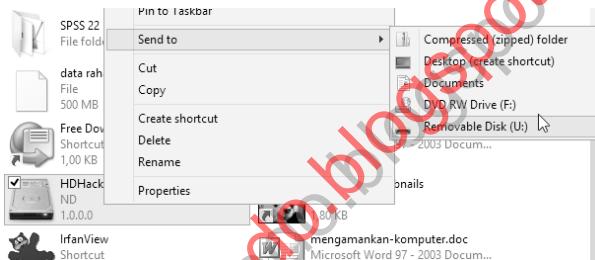
Gambar 9.27 Tampilan Properties dari file Removable disk

9. Jika Anda lihat file kontainer tersebut di Windows Explorer, maka terlihat ukuran file tersebut sesuai saat dibuat. Walaupun isinya masih kosong, tapi kontainer tersebut ukurannya sudah fix.



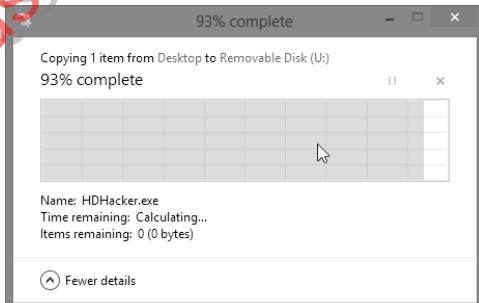
Gambar 9.28 File dari volume terenkripsi

10. Drive yang sudah ter-mount dapat diperlakukan seperti harddisk biasa, antara lain Anda dapat memindahkan file ke drive tersebut.



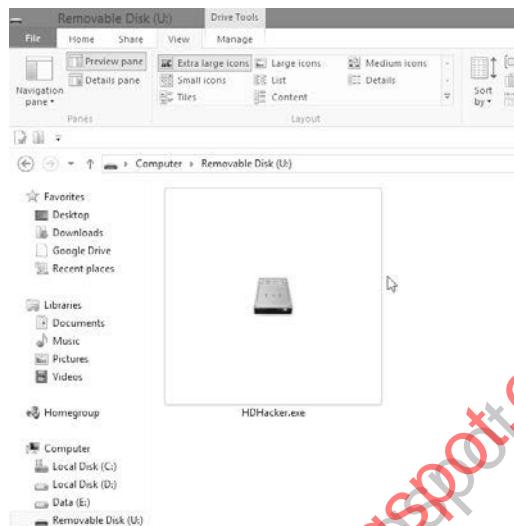
Gambar 9.29 Memindahkan sebuah folder ke Removable disk hasil mounting

11. Proses penyalinan pun berlangsung seperti biasa, misalnya dengan adanya box **Copying** seperti gambar berikut.



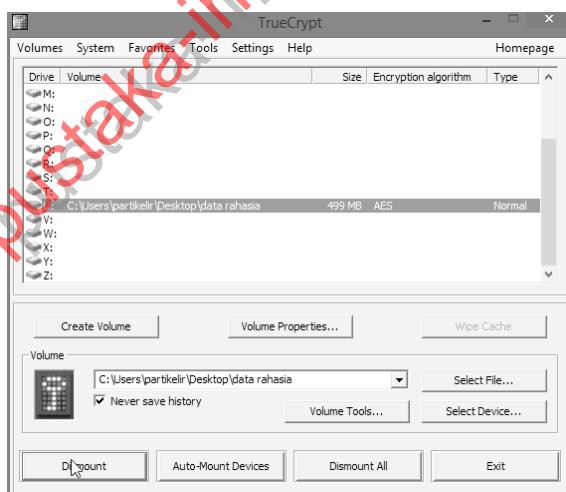
Gambar 9.30 Box Copying yang menjelaskan bahwa proses penyalinan ke drive Removable disk sedang berlangsung

12. Ketika drive hasil mounting dibuka, maka terlihat file pun sudah tersalin dengan benar.



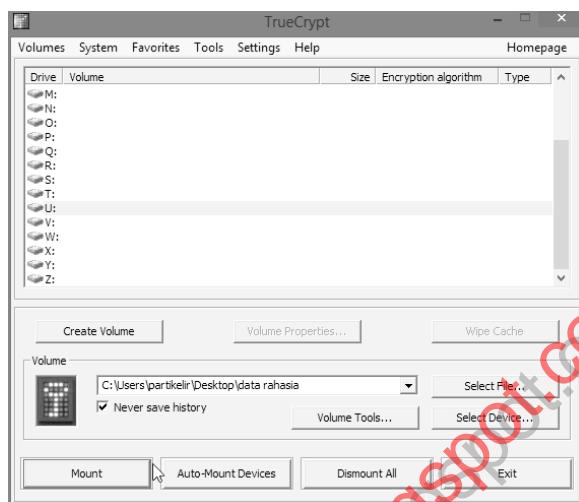
Gambar 9.31 File sudah tersalin dengan benar

13. Untuk melepas mounting, Anda tinggal memilih drive yang ada di window utama dari aplikasi TrueCrypt, kemudian klik button **Dismount**.



Gambar 9.32 Klik pada button Dismount untuk melepas mounting

14. Setelah tidak di-mount, nama drive tidak terlihat lagi ada tulisan di kolom Volume pada nama drive yang bersangkutan di window utama TrueCrypt.



Gambar 9.33 Window utama TrueCrypt

15. Di Windows Explorer pun terlihat tidak ada drive lagi, ini disebabkan karena mounting sudah dilepas.



Gambar 9.34 Windows Explorer sudah tidak melihat adanya drive Removable disk (U) karena sudah dilepas mount-nya

## BAB 10

# Membantai Spyware

Spyware adalah salah satu ancaman komputer yang terkait dengan internet. Dilihat dari jenisnya, spyware merupakan sebuah software yang diinstal secara rahasia ke dalam komputer tanpa disadari user. Tujuannya adalah mengambil data dari komputer untuk berbagai keperluan.

Spyware artinya software mata-mata. Namun, tidak hanya memata-matai user, software ini bisa mengumpulkan berbagai informasi penting seperti kebiasaan berinternet, situs-situs yang dikunjungi, atau bahkan memengaruhi kinerja komputer.

Spyware bisa melakukan penginstalan software tambahan (selain spyware utama), lalu bisa juga memerintahkan browser untuk membuka halaman tertentu. Spyware juga umumnya mengubah setting komputer yang memungkinkan koneksi internet melambat, atau bahkan memakan memory, sehingga penggunaan komputer untuk keperluan kerja juga terhambat.

Spyware umumnya akan mempengaruhi proses berinternet, atau secara praktis akan mempengaruhi cara kerja browser. Misalnya dengan mengubah alamat homepage dari browser yang dibuka tiap browser pertama kali dibuka.

## **10.1 Mengenal Spyware**

Spyware sangat mengganggu, karena itu muncullah banyak pembuat software yang kemudian memutuskan mengembangkan software anti spyware untuk menghalangi spyware diinstal dan mencuri data dari komputer Anda.

Software anti spyware ini merupakan teknik yang disarankan untuk melindungi komputer Anda. Tidak seperti virus atau worm, umumnya spyware tidak menduplikasikan diri.

Namun, spyware juga tidak kalah berbahayanya. Karena spyware akan mengeksplorasi komputer untuk keperluan komersil. Umumnya teknik yang digunakan oleh spyware adalah memunculkan popup berupa iklan, mencuri informasi rahasia (seperti akun bank, email, dan sebagainya), lalu memonitor browsing untuk nantinya data-data tersebut dikumpulkan untuk keperluan marketing.

Bagaimana tanda bahwa komputer Anda terkena spyware? Tidak ada yang bisa mengetahuinya dengan pasti jika belum menginstal software anti spyware. Namun, jika komputer terasa lambat padahal Anda tak menginstal software apa pun, kemungkinan ada spyware di komputer Anda.

Selain itu, jika tiba-tiba Anda mem-buka halaman web tertentu padahal Anda tidak merasa mengetikkan URL halaman tersebut, maka kemungkinan itu adalah efek dari spyware.

Spyware adalah sebuah program komputer yang masuk ke komputer tanpa izin. Setelah masuk, mereka akan menyedot kemampuan pemrosesan di komputer Anda.

Berapa sebenarnya jumlah infiltrasi spyware di komputer? Para pengamat mengatakan bahwa kira-kira hampir 80% pengguna komputer di dunia terjangkiti spyware, walaupun beberapa orang tak menyadarinya.

Beberapa orang menyangka spyware adalah virus komputer. Padahal prinsipnya beda. Virus adalah kode yang mereplikasi diri dari satu komputer ke komputer lainnya dan tujuannya adalah merusak file dan sistem operasi komputer.

Tapi spyware berbeda metodenya, spyware tidak ingin merusak komputer, mereka hanya ingin mengambil data-data penting di komputer untuk keperluan marketing ilegal. Spyware masuk ke komputer secara diam-diam, kemudian berjalan di background.

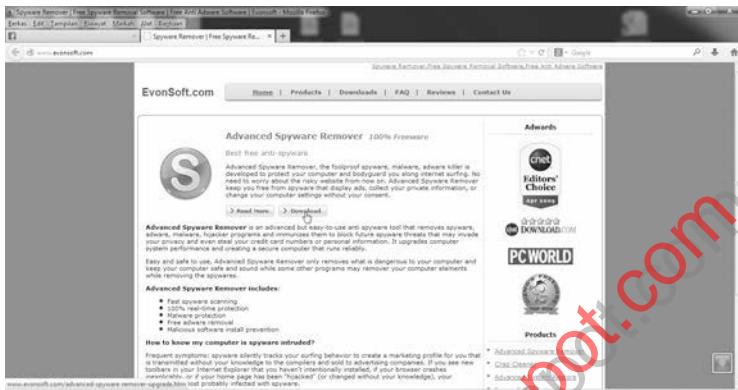
Jadi, tidak ada kerusakan fisik karena spyware, Anda masih bisa mengetik, membuat spreadsheet, atau bekerja seperti hari-hari biasanya. Namun, data Anda akan dicuri. Karena itu spyware juga dianggap mengganggu sama seperti virus komputer.

Ada beberapa metode bagaimana spyware bisa masuk ke komputer. Berikut ini beberapa penjelasannya:

- Mendompleng instalasi software utama: Salah satu modus masuknya spyware adalah dengan mendompleng pada instalasi software utama. Beberapa software gratisan yang menyediakan iklan biasanya memiliki misi spyware di belakangnya. Misalnya, software sharing P2P seperti Kazaa diklaim menginstalkan spyware di dalamnya.
- Download: Sering kali, ketika Anda download file, otomatis muncul jendela popup yang meminta Anda menginstal software di komputer. Beberapa browser kadang bahkan bisa menginstalkan software tersebut otomatis. Karena itu, pastikan gunakan browser yang secure untuk mencegah hal ini.
- Melalui plugin Browser: Beberapa plugin dari browser merupakan spyware yang bisa mencuri data Anda di dalamnya. Karena itu, berhati-hati ketika menginstal plugin atau add-ons di browser Anda. Siapa tahu itu spyware, pastikan Anda download dari sumber yang terpercaya.
- Dari software anti-spyware: Ya, beberapa software anti-spyware yang seharusnya mematikan spyware justu merupakan spyware. Ini ibarat maling teriak maling. Karena itu, berhati-hatilah ketika memilih anti-spyware, pastikan anti-spyware yang digunakan merupakan software yang bonafide.

## 10.2 Advanced Spyware Remover

Salah satu software yang punya legitimasi sebagai anti spyware yang handal namun free adalah Advanced Spyware Remover dari <http://www.evonsoft.com/>.



Gambar 10.1 Situs untuk download Advanced Spyware Remover

Untuk menggunakan software ini, pertama kali Anda harus menginstalnya di komputer Anda terlebih dahulu.

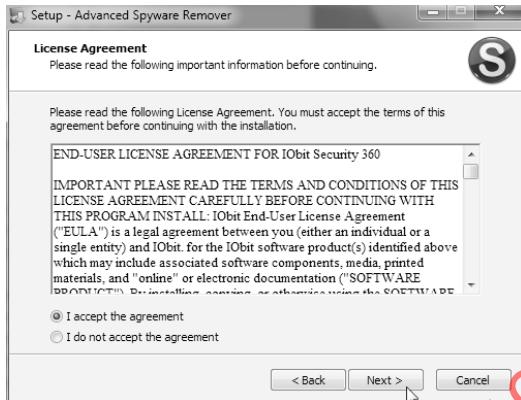
Berikut ini langkahnya:

1. Eksekusi installer Advanced Spyware Remover. Kemudian klik button Next di window Welcome to the Advanced Spyware Remover Setup Wizard.



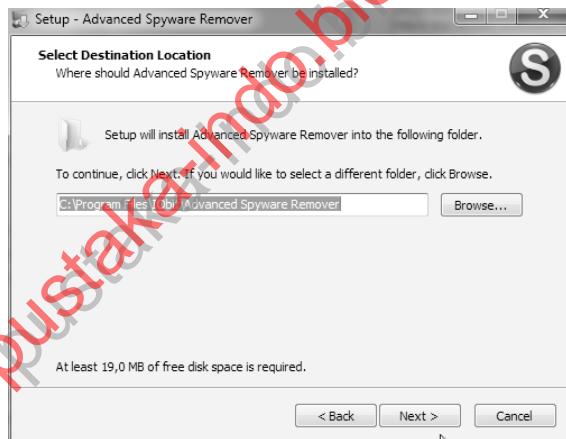
Gambar 10.2 Jendela Welcome to the Advanced Spyware Remover

2. Pilih radio button **I accept the agreement** di window License Agreement dan klik button Next.



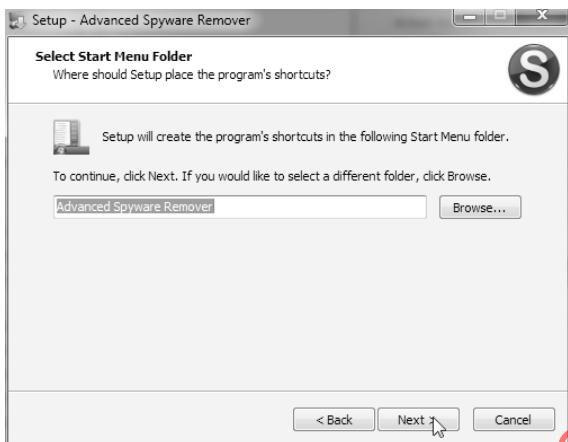
Gambar 10.3 Setujui License Agreement

3. Pilih lokasi instalasi Advanced Spyware Remover di textbox pada window Select Destination Location. Klik button Next.



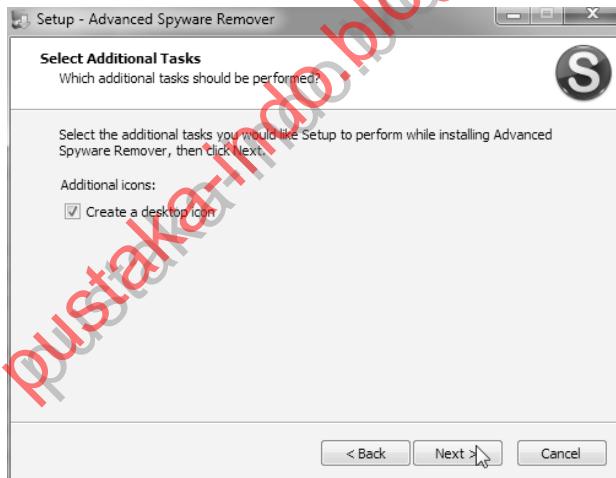
Gambar 10.4 Select Destination Location  
untuk memilih lokasi instalasi

4. Isikan nama untuk start menu yang diperlukan untuk mengakses Advanced Spyware Remover ini di window Select start menu folder. Klik Next untuk melanjutkannya ke langkah berikutnya.



*Gambar 10.5 Select Start menu folder untuk menentukan nama folder Start menu*

- Untuk **Additional Tasks**, Anda dapat menentukan apakah instalasi akan membuatkan ikon desktop. Klik button **Next** untuk melanjutkan lagi.



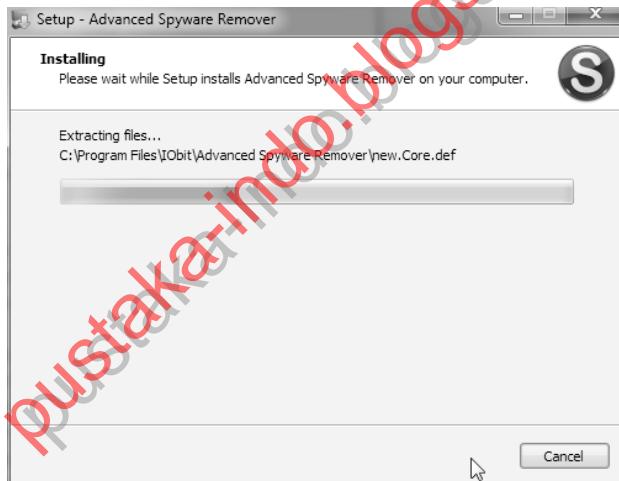
*Gambar 10.6 Select Additional task untuk membuat ikon di Desktop dan quick launch*

- Setelah semuanya dipilih, atribut instalasi ditampilkan di jendela **Ready to Install**. Kemudian, klik button **Install** untuk melakukan instalasi.



**Gambar 10.7 Klik pada button *Install* untuk melakukan instalasi**

7. Tunggu hingga instalasi Advanced Spyware Remover ini sudah selesai.



**Gambar 10.8 Proses instalasi Advanced Spyware Remover**

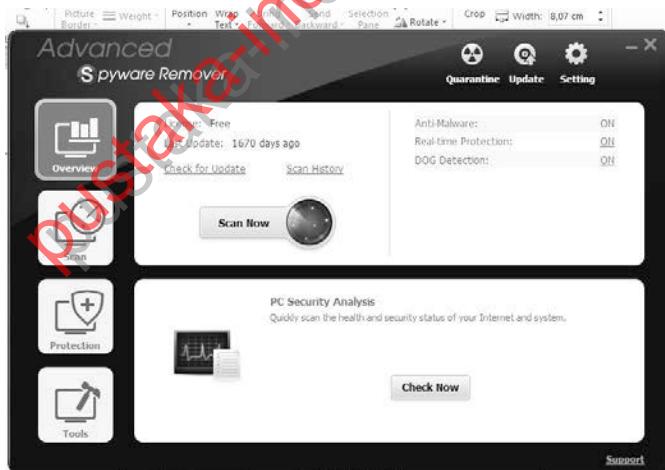
8. Terakhir, klik **Finish** di window **Completing the Advanced Spyware Remover Setup Wizard**.



**Gambar 10.9 Instalasi Advanced Spyware Remover Free Edition selesai**

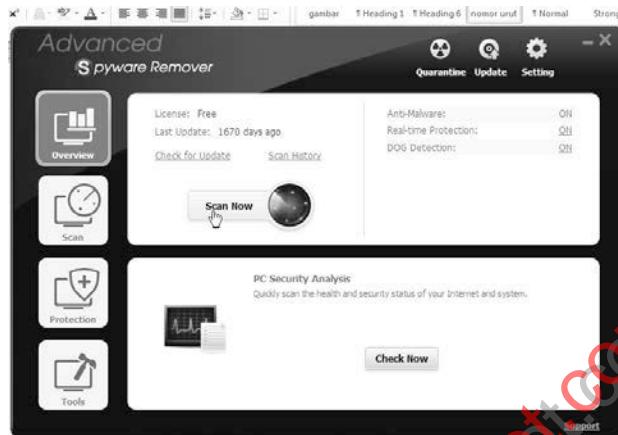
Setelah itu, Anda dapat menggunakan Spyware Remover yang telah diinstal di atas. Cara penggunaanya sangat mudah. Berikut ilustrasi penggunaan Advanced Spyware Remover untuk menghilangkan spyware di komputer Anda:

1. Jalankan Advanced spyware remover. Tampilan jendela utama ASR ini seperti berikut.



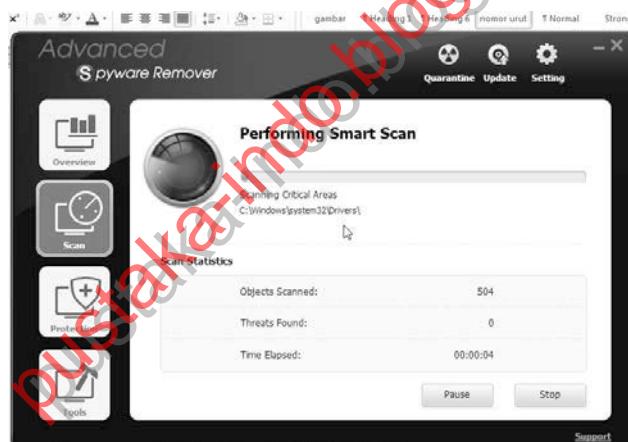
**Gambar 10.10 Window utama Advaned Spyware remover**

2. Klik pada **Scan now** untuk memindai pertama kali komputer Anda dari spyware.



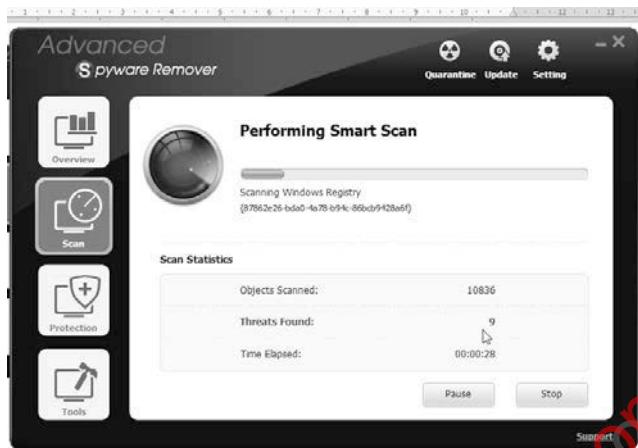
Gambar 10.11 Klik **Scan now**

3. Tunggu hingga scan berlangsung.



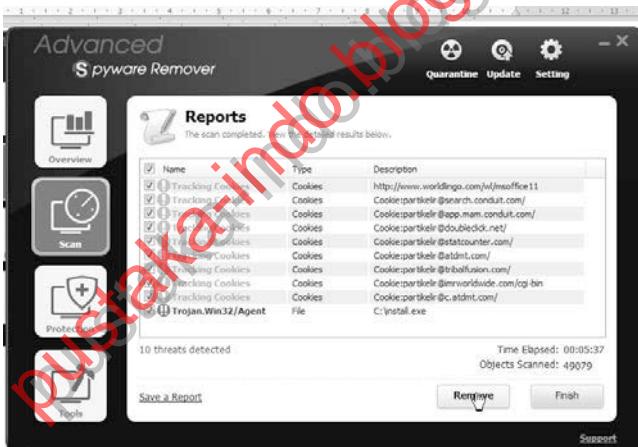
Gambar 10.12 Scan tengah berlangsung

4. Ketika scan mengetahui ada ancaman spyware, muncul jumlah ancaman ini di **Threats found**.



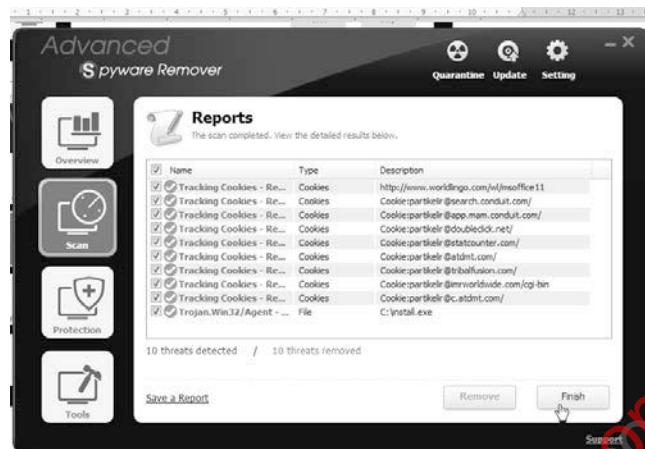
Gambar 10.13 Threats found menunjukkan ada ancaman

5. Kalau pemindaian sudah selesai, ancaman-ancaman akan ditampilkan di reports. Cek pada semua ancaman ini, kemudian klik Remove untuk menghapusnya.



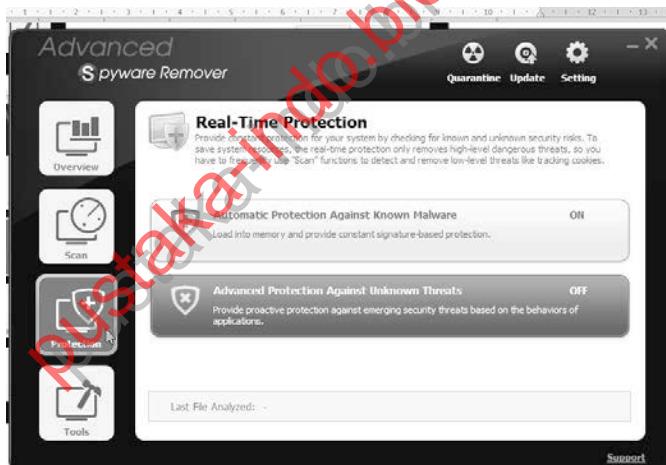
Gambar 10.14 Klik Remove untuk menghapus report

6. Kalau sudah terhapus, maka status menjadi hijau, klik Finish.



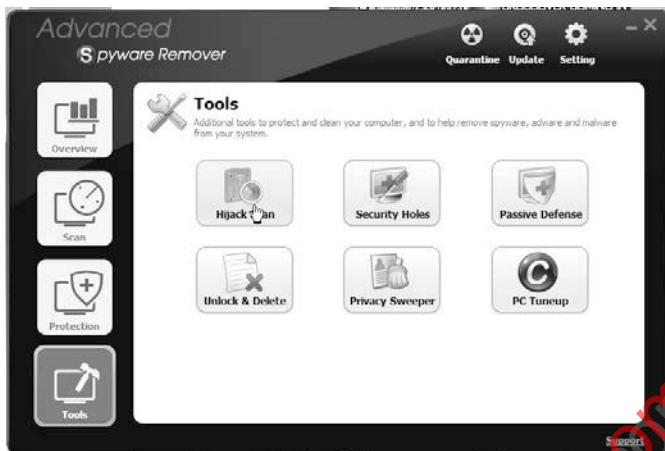
Gambar 10.15 Ancaman sudah terhapus

7. Di **Protection**, Anda dapat mengaktifkan atau mematikan Real time protection yang akan membuat program ini berjalan di background dan melihat apakah ada ancaman atau tidak.



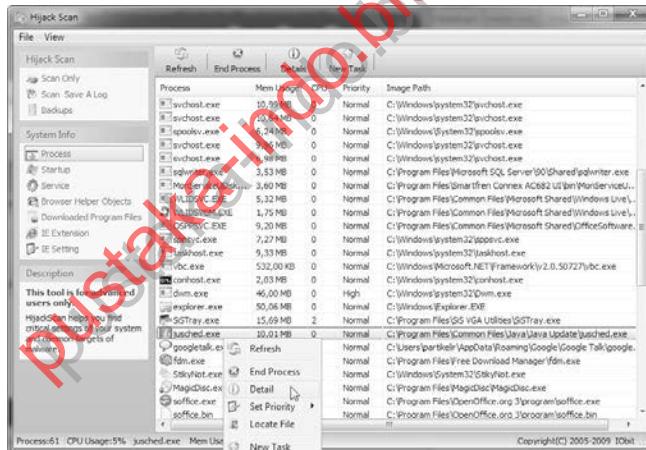
Gambar 10.16 Tab Protection

8. Klik **Tools** untuk menyingkap berbagai tool yang disediakan. Hijack scan untuk melihat aplikasi dan proses yang berjalan.



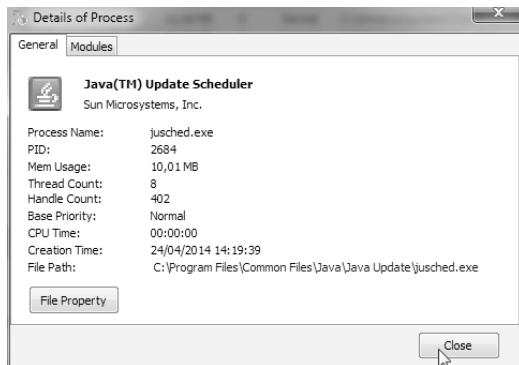
Gambar 10.17 Klik pada Hijack scan

9. Maka, terlihat aplikasi dan proses yang muncul, sama seperti Task Manager, tapi lebih detil. Anda bisa mengklik kanan pada salah satu proses, kemudian klik **Detail** untuk melihat detailnya.



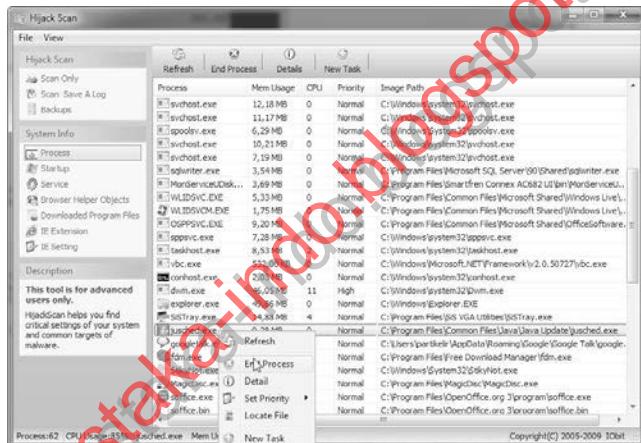
Gambar 10.18 Klik kanan pada salah satu proses

10. Anda bisa melihat detail process, termasuk nama proses, PID, penggunaan memory, prioritas, CPU time, dan sebagainya.



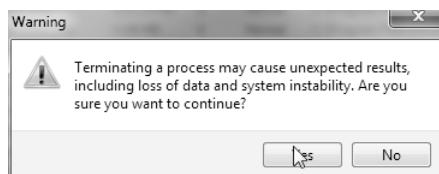
Gambar 10.19 Detail proses

11. Anda juga bisa mematikan proses tertentu dengan klik kanan, kemudian pilih menu **End process**.



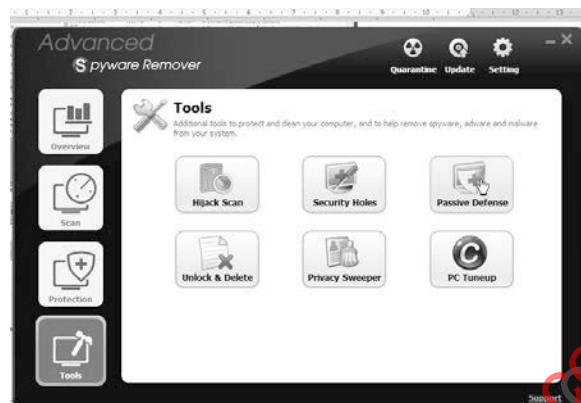
Gambar 10.20 End process untuk mengakhiri proses

12. Muncul konfirmasi apakah hendak mengakhiri proses, klik Yes.



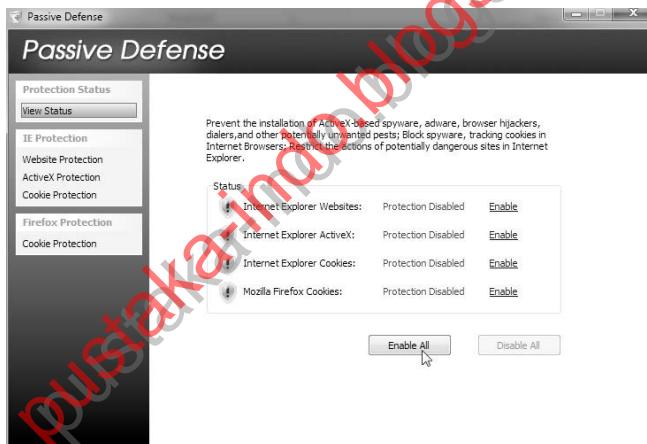
Gambar 10.21 Konfirmasi apakah hendak mengakhiri proses

13. Kembali ke Tools, klik **Passive Defense** untuk mengaktifkan **Passive Defense**.



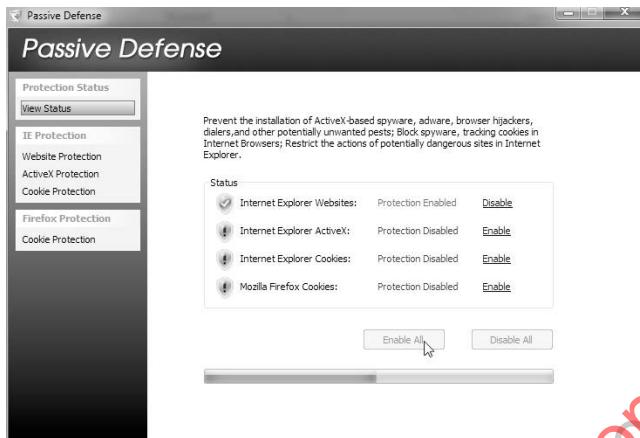
Gambar 10.22 Klik pada Passive Defense

14. Klik **Enable All** untuk mengaktifkan **Passive Defense** ini.



Gambar 10.23 Mengaktifkan Passive Defense

15. Tunggu hingga semua fitur proteksi **Passive Defence** diaktifkan. Ini memakan waktu yang agak lama.



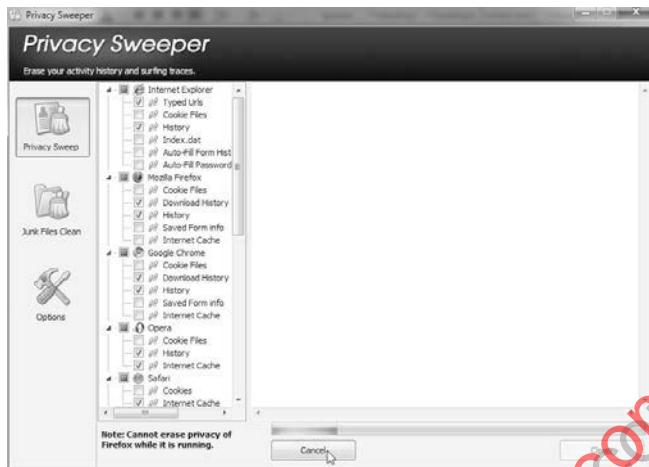
Gambar 10.24 Fitur proteksi Passive Defense

16. Kalau ada cookies atau apa pun di komputer yang bisa mencuri data privacy Anda, klik pada **Privacy Sweeper** di kotak Tools.



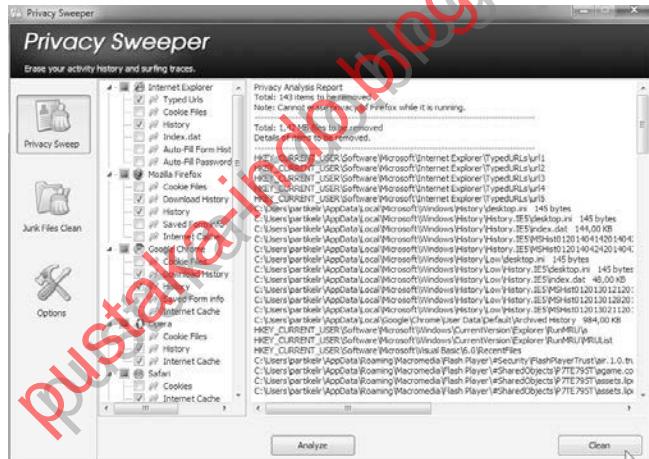
Gambar 10.25 Privacy sweepers

17. Pindai dengan klik **Scan**.



Gambar 10.26 Memindai privacy items

18. Semua file yang berpotensi mencuri privacy akan ditampilkan, klik **Clean** untuk menghapus semuanya.



Gambar 10.27 Klik **Clean** untuk menghapus ancaman privacy

19. Kalau sudah, muncul tulisan **Cleaning completed** yang menunjukkan pembersihan sudah optimal.



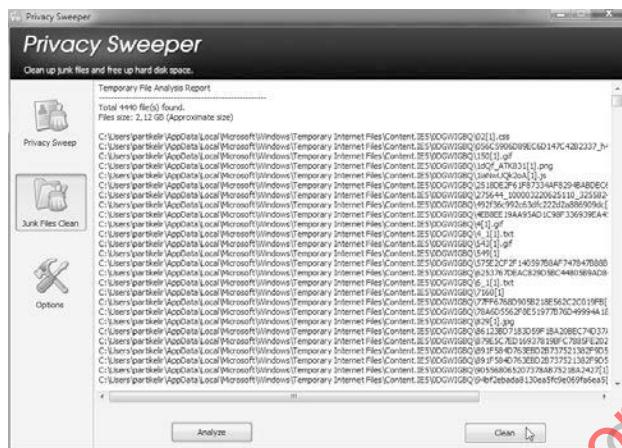
Gambar 10.28 Informasi Cleaning completed

20. Klik tombol **Junk files clean** dan klik **Scan**.



Gambar 10.29 Scanning pada Junk files clean

21. Kalau telah terpindai semua, klik **Clean**.



Gambar 10.30 Membersihkan junk file

# BAB 11

## Clean Uninstall

Beberapa software yang tak baik perlakunya umumnya membandel pula ketika hendak di-uninstall. Bisa jadi, software tersebut tidak hilang sepenuhnya dari komputer walaupun sudah melalui proses uninstall yang dibawa oleh software tersebut. Atau malah sama sekali tidak terlihat di window **Add/Remove Programs** di Control Panel.

Untuk menangani program-program yang membandel ini, Anda bisa menggunakan beberapa program clean uninstall. Salah satu software ini adalah Revo uninstaller dari [www.revouninstaller.com](http://www.revouninstaller.com).

### 11.1 Uninstall dengan Revo Uninstaller

Revo Uninstaller adalah software untuk melakukan clean uninstall. Dengan software ini, software-software yang masih menyisakan file di komputer, atau di registry bisa dibabat habis. Versi Revo uninstaller yang 2 varian (salah satunya adalah Portabel) memungkinkan Anda untuk tak perlu menginstal software ini.

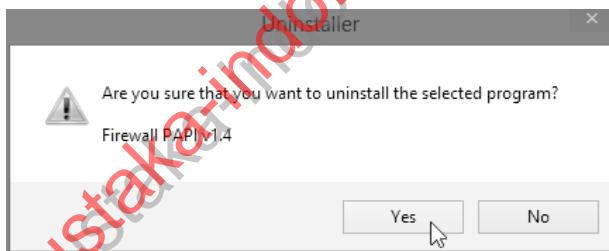
Tinggal ekstrak, maka software ini siap untuk dipakai. Berikut ini contoh bagaimana meng-uninstall program menggunakan Revo uninstaller:

1. Perhatikan halaman muka **Revo uninstaller** seperti gambar berikut, klik dua kali pada nama program yang ingin di-uninstall di komputer Anda.



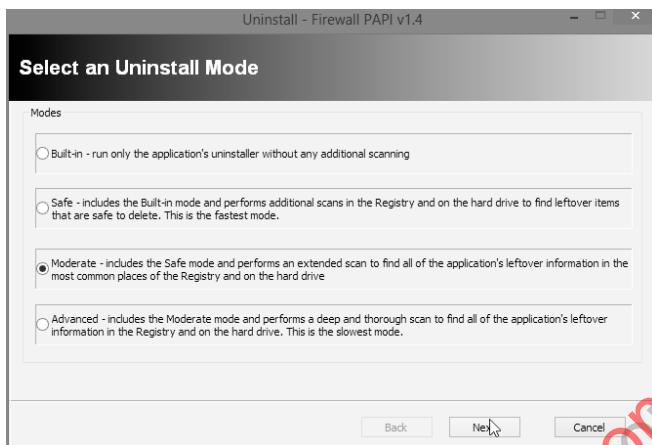
Gambar 11.1 Klik dua kali pada nama program untuk di-uninstall

2. Muncul box konfirmasi **Are you sure that you want to uninstall the selected program?** Klik pada button **Yes**.



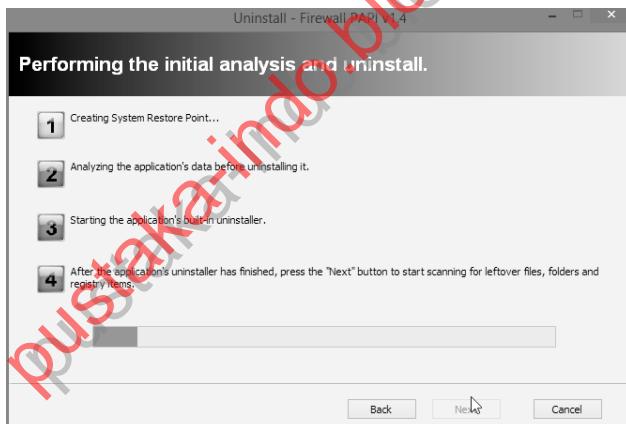
Gambar 11.2 Konfirmasi **Are you sure that you want to uninstall the selected program**

3. Mode uninstall ada 4 di **Revo Uninstaller**. Anda dapat memilih yang **Moderate** yang merupakan mode uninstall standar. Klik pada button **Next**.



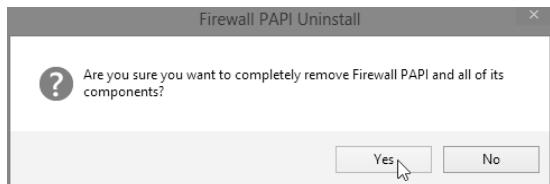
Gambar 11.3 Pemilihan metode uninstall

4. Maka, proses analisis dan uninstall dimulai. Ada 4 tahap di sini, yaitu membuat system restore point, menganalisis data, memulai aplikasi uninstall bawaan dari program, lalu proses lanjutan setelah uninstall.



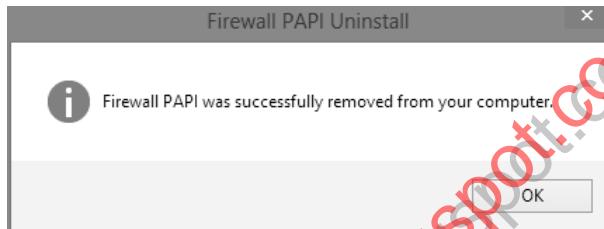
Gambar 11.4 Tahap Creating System Restore point

5. Ketika proses uninstall dari program dijalankan, Anda melihat box yang menjelaskan aplikasi-aplikasi uninstall, yang pertama biasanya konfirmasi **Are you sure you want to completely remove nama\_program**. Klik saja button Yes.



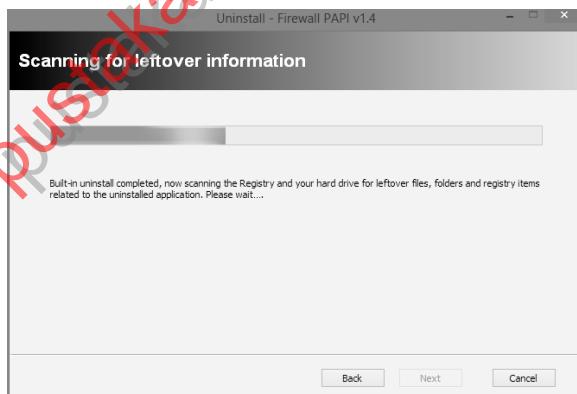
**Gambar 11.5 Box konfirmasi untuk uninstall program melalui proses uninstall default bawaan produk tersebut**

6. Proses uninstall bawaan produk akan terlihat seperti berikut.



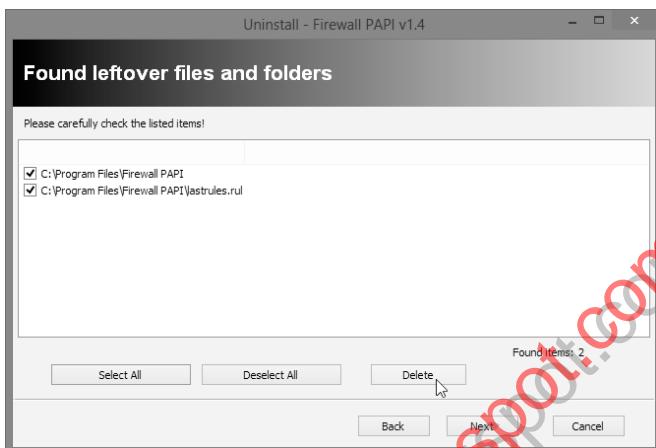
**Gambar 11.6 Proses uninstall bawaan dari software**

7. Setelah selesai, Anda tinggal mengklik Next di window **Performing the initial analysis and uninstall**.
8. Revo akan memindai apakah ada sisa-sisa file di registry yang berkaitan dengan software yang barusan di-uninstall tersebut.



**Gambar 11.7 Proses pemindaian dari informasi yang belum terhapus dari komputer**

9. Fasilitas uninstaller bawaan software tersebut umumnya tidak komplit dalam membersihkan registry. Pilih semua informasi yang tersisa dengan mengklik button **Select All**, kemudian klik pada button **Delete** untuk menghapusnya.



Gambar 11.8 Penghapusan semua informasi di Regedit

10. Kalau sudah di akhir, klik button **Finish** di window **Finish**. Artinya, file sudah benar-benar hilang dari komputer Anda dengan bersih.

*pusatka-indo.blogspot.com*

# Tentang Penulis

## **Edy Winarno ST, M.Eng**

Penulis adalah staf pengajar di Universitas Stikubank Semarang. Pendidikan terakhirnya adalah Master of Engineering (M.Eng.) Computer & Informatics System di Teknik Elektro Universitas Gadjah Mada (UGM). Selain mengajar, penulis juga berkecimpung di dunia blogging dan sedikit melakukan entrepreneurship.

## **Ali Zaki**

Penulis adalah seorang pekerja TI di bidang pemrograman, multimedia, dan web. Saat ini menjadi outsourcee untuk sebuah perusahaan konsultan TI di Jakarta. Penulis bekerja secara remote melalui SOHO di rumahnya di Semarang. Di sela-sela aktivitasnya, penulis juga aktif melakukan penulisan buku di komunitas SmitDev. Beberapa karya buku penulis telah diterbitkan oleh Elex Media Komputindo.

## **SmitDev Community**

SmitDev merupakan lembaga komunitas yang menjadi wadah bagi para praktisi teknologi informasi dan komputer. Salah satu aktivitas SmitDev saat ini adalah melakukan penulisan buku komputer dan mempersembahkan karya buku bagi kalangan pengguna dan peminat bidang teknologi informasi dan komunikasi di tanah air.

Pembaca dapat menyampaikan saran, tanggapan, dan pertanyaan melalui layanan forum interaksi pembaca yang tersedia di <http://www.smitdev.com>, atau melalui email [info@smitdev.com](mailto:info@smitdev.com).

**Catatan:**

- Untuk melakukan pemesanan buku, hubungi Layanan Langsung PT Elex Media Komputindo:

**Gramedia Direct**

Jl. Palmerah Barat No. 33, Jakarta 10270

Telemarketing/CS: 021-53650110/111 ext: 3901/3902

Email: **endang@gramediapublishers.com**

[pustaka-indo.blogspot.com](http://pustaka-indo.blogspot.com)

# PENGAMANAN PC

## dari Segala Ancaman

Komputer ibarat rumah, jika rumah bisa kecurian, maka komputer bisa mendapatkan ancaman dari pihak luar. Karena itu, kewaspadaan merupakan hal wajib yang harus diperhatikan oleh semua pemilik komputer.

Banyak pemilik komputer yang tidak menyadari bahwa perlu adanya perhatian khusus dalam masalah keamanan komputer. Buku ini menjelaskan bagian penting yang harus diperhatikan untuk menjaga keamanan komputer dari berbagai gangguan, serta meningkatkan keamanan dari sistem komputer rumah.

Setelah mempelajari buku ini, diharapkan Anda akan mampu menjauhkan komputer dari semua ancaman, sehingga komputer Anda aman terkendali.

Pembahasan lebih lengkap meliputi:

- Pengamanan dengan firewall dan antivirus
- Menghindari berbagai ancaman online dan email
- Up to date dengan patch
- Backup dan restore PC
- Menggunakan enkripsi dan password
- Tips download yang aman
- Membantai spyware
- Clean uninstall software



gramedia

Penerbit PT Elex Media Komputindo  
Kompas Gramedia Building  
Jl Palmerah Barat 29-37  
Jakarta 10270  
Telp. (021) 53650110, 53650111 ext. 3214  
Web Page: <http://www.elexmedia.co.id>

Kelompok
Utility
Keterampilan
<input checked="" type="checkbox"/> Tingkat Pemula
<input checked="" type="checkbox"/> Tingkat Menengah
<input type="checkbox"/> Tingkat Mahir
Jenis Buku
<input checked="" type="checkbox"/> Referensi
<input checked="" type="checkbox"/> Tutorial
<input type="checkbox"/> Latihan

ISBN 978-602-02-4374-0



9 786020 243740

121141463