



Tips & Trik Keamanan Windows 8 & 8.1

Vyctoria

Tips & Trik Keamanan Windows 8 & 8.1

Sanksi Pelanggaran Pasal 72:
Undang-Undang Nomor 19 Tahun 2002
Tentang Hak Cipta

1. Barangsiapa dengan sengaja melanggar dan tanpa hak melakukan perbuatan sebagaimana dimaksud dalam Pasal 2 Ayat (1) atau Pasal 49 Ayat (1) dan Ayat (2) dipidana dengan pidana penjara masing-masing paling singkat 1 (satu) bulan dan/atau denda paling sedikit Rp 1.000.000,00 (satu juta rupiah), atau pidana penjara paling lama 7 (tujuh) tahun dan/atau denda paling banyak Rp 5.000.000.000,00 (lima milyar rupiah).
2. Barangsiapa dengan sengaja menyiarkan, 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 Rp 500.000.000,00 (lima ratus juta rupiah).

Tips & Trik Keamanan Windows 8 & 8.1

Vyctoria

PENERBIT PT ELEX MEDIA KOMPUTINDO



KOMPAS GRAMEDIA

Tips & Trik Keamanan Windows 8 & 8.1

Vyctoria

© 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

121142602

ISBN: 978-602-02-5475-3

[eEp]

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

Perkembangan sistem operasi terus maju, saat ini sistem operasi terbaru adalah Windows 8, dan juga varians-nya Windows 8.1. Sistem keamanan sistem operasi juga terus meningkat demi keamanan dan kenyamanan para *user*-nya. Dalam Windows 8 ada banyak sistem keamanan yang telah disediakan. Namun, apabila kita tidak bisa menggunakananya secara optimal, tentu saja semua fasilitas tersebut menjadi terbengkalai dan pajangan saja.

Dalam buku ini akan membedah secara tuntas sistem keamanan yang diterapkan pada Windows 8, dan juga Windows 8.1. Selain penjelasan secara konsep maka akan dijelaskan pula langkah-langkah praktis untuk menggunakan fitur keamanan yang disediakan tersebut yang tentu saja untuk mengamankan komputer maupun laptop/netbook Anda. Tidak hanya cara pemakaiannya saja, Anda juga akan belajar bagaimana mengoptimalkan fungsi sistem keamanan tersebut sehingga komputer Anda menjadi lebih aman. Buku ini juga disertai dengan berbagai tips dan trik kemanan yang perlu Anda ketahui.

Apa yang dijelaskan dalam buku ini akan membedah sistem pengamanan pada Windows 8 tanpa melibatkan pemakaian program dari pihak ketiga, jadi para pembaca dijamin tidak perlu mendownload program tambahan apapun. Karena semuanya sudah disediakan oleh Windows 8. Beberapa fitur pengamanan, bukan hanya memasang password belaka, dan mencegah virus saja. Lebih dari itu, buku ini juga akan menjelaskan bagaimana Anda bisa memonitor pemakaian komputer terutama oleh anak-anak Anda supaya tidak membuka website yang negatif serta menjalankan aplikasi yang dilarang. Bagaimana cara kita bisa mengatasi lupa password dengan fasilitas *reset disk*. Begitu pula dalam pemasangan password tidak hanya berupa kata-

kata yang selama ini kita kenal, juga tersedia password dalam bentuk gambar dan PIN.

Lebih dalam lagi, buku ini akan menunjukkan kepada Anda bagaimana cara data di dalam komputer Anda menjadi aman sehingga tidak bisa dibuka oleh orang lain. Jangankan membuka, menyalinnya ke dalam flashdisk saja juga tidak akan bisa. Begitu pula dengan memanfaatkan sistem Recovery yang akan membantu Anda ketika ada masalah dengan Windows, bukan hanya System Restore yang selama ini sudah dikenal. Karena dalam Windows 8 juga ada fasilitas untuk *refresh* dan *reset* Windows yang tidak pernah pada sistem operasi sebelumnya.

Dalam buku ini pula, Anda akan mengenal apa itu *Data Execution Prevention*, dan juga *SmartScreen*. Ada banyak hal lainnya yang akan dibahas dalam buku ini seputar sistem keamanan Windows 8 dan Windows 8.1. Belum lagi, buku ini juga menyediakan sebuah bab khusus yang berisikan berbagai trik seputar sistem keamanan lainnya. Bahkan dalam setiap bab juga telah disertai sebuah tips singkat dalam hal keamanan Windows.

Tidak semua gambaran bisa terpenuhi dalam kata pengantar ini karena semua sistem pengamanan akan kupas secara tuntas dalam buku. Anda harus menyelaminya sendiri. Semoga buku ini dapat menjadi referensi yang berguna bagi Anda. Dan selamat membedah *Sistem Keamanan Windows 8 & Windows 8.1*.

DAFTAR ISI

KATA PENGANTAR.....	V
DAFTAR ISI	VII
BAB 1 PENDAHULUAN.....	1
BAB 2 MENGELOLA USER ACCOUNTS.....	3
2.1 Menambah Account	7
2.2 Mengubah Nama Account.....	10
2.3 Mengubah Status Account	11
2.4 Memasang Password.....	13
2.5 Mengganti Password	15
2.6 Menghapus Account.....	16
2.7 User Account Control	19
2.8 Tips.....	24
BAB 3 MICROSOFT ACCOUNT	27
3.1 Mendaftar Account	28
3.2 Beralih ke Microsoft Account.....	30
3.3 Picture Password	33
3.4 Menggunakan PIN.....	37
3.5 Kembali ke Local Account.....	38
BAB 4 PASSWORD RESET DISK.....	41
4.1 Membuat Password Reset Disk.....	42
4.2 Menggunakan Password Reset Disk	45
4.3 Tips.....	48
BAB 5 FAMILY SAFETY & EVENT VIEWER.....	49
5.1 Membatasi Akses Website	51
5.2 Mengatur Waktu Pemakaian Komputer	55

5.3	Batasan Pemakaian Windows Store dan Game	57
5.4	Memblokir Aplikasi	62
5.5	Melihat Aktivitas Pemakaian.....	63
5.6	Event Viewer.....	65
5.7	Tips.....	69
BAB 6	KEAMANAN FILE DAN FOLDER.....	71
6.1	Melarang Akses File & Folder	73
6.2	Enkripsi File & Folder.....	75
6.3	Backup Key Enkripsi	80
6.4	Menggunakan Key Enkripsi	88
6.5	Tips.....	91
BAB 7	WINDOWS DEFENDER	93
7.1	Scan Malware	95
7.2	Real-time Protection.....	98
7.3	Melihat Hasil Temuan Windows Defender.....	99
7.4	Update Windows Defender	103
7.5	Tips.....	106
BAB 8	WINDOWS FIREWALL.....	109
8.1	Mengatur Program Melalui Firewall.....	111
8.2	Windows Firewall with Advanced Security.....	114
8.3	Inbound & Outbound Rules.....	117
8.4	Menutup Port	119
8.5	Tips.....	121
BAB 9	FILE HISTORY	123
9.1	Membackup Data.....	125
9.2	Mengembalikan Data.....	128
9.3	Mempercepat Proses Backup	131
9.4	Tips.....	133
BAB 10	RECOVERY	135
10.1	Membuat Recovery Drive	136
10.2	Refresh Windows.....	138
10.3	Melihat System Restore	142
10.4	Konfigurasi System Restore.....	146
10.5	Membuat Restore Point	148
10.6	Tips.....	150
BAB 11	SYSTEM CONFIGURATION	155
11.1	General	156
11.2	Startup	157

11.3	Boot.....	159
11.4	Services.....	161
11.5	Tools.....	163
11.6	Tips.....	164
BAB 12	DATA EXECUTION PREVENTION	169
12.1	Memasang Program pada Daftar DEP	172
12.2	Mematikan DEP	174
12.3	Tips.....	177
BAB 13	PENTINGNYA WINDOWS UPDATE.....	179
13.1	Memeriksa Status Windows Update.....	182
13.2	Melihat History Update	183
13.3	Restore Hidden Update	185
13.4	Memilih Update	186
13.5	Tips.....	188
BAB 14	LOCAL GROUP POLICY EDITOR	189
14.1	Melarang Akses Control Panel	190
14.2	Menampilkan Konfirmasi Penghapusan.....	193
14.3	Menampilkan Seluruh Konfigurasi	195
14.4	Menyembunyikan Tab Security.....	196
BAB 15	KONFIGURASI SMARTSCREEN	201
BAB 16	TRIK KEAMANAN TAMBAHAN.....	207
16.1	Screen Saver Sebagai Pengaman	207
16.2	Safe Mode pada Windows 8	210
16.3	Mencari Versi Windows.....	215
16.4	Mencegah Penularan Virus	216
16.5	Virtual Drive.....	217
TENTANG PENULIS		221

1

PENDAHULUAN

Sebelum Anda meneruskan membaca bagian selanjutnya, sebaiknya Anda membaca paragraf pertama ini terlebih dahulu. Perlu diketahui, apabila dalam buku ini saya menyebutkan Windows 8, hal itu berarti sudah mencakup Windows 8 dan Windows 8.1. Sebab terlalu boros kalau kedua nama tersebut harus saya sebutkan bolak-balik. Selain itu, apabila dalam buku ini disebutkan kata “komputer” hal ini bukan berarti Windows 8 yang diinstall pada komputer saja, melainkan semua perangkat lainnya yang menginstall Windows 8 dan Windows 8.1, termasuk juga Laptop/Notebook, Netbook, komputer server dan sebagainya. Sehingga untuk mewakili semua perangkat tersebut maka saya akan menyebutnya dengan nama komputer saja.

Windows 8 hadir dengan berbagai sistem keamanan yang tidak hanya untuk mengamankan data dalam komputer Anda saja. Ada banyak manfaat lainnya ketika kita bisa mengetahui berbagai kelebihan Windows 8 melalui sistem keamanan yang terdapat di dalamnya. Sebagai pengantar dan bab pertama dalam buku ini akan mengawali langkah Anda sebelum membedah sistem keamanan yang terdapat pada Windows 8.

Windows 8 telah menyediakan berbagai fasilitas atau fitur keamanan yang bisa dimanfaatkan oleh usernya. Apabila kita tidak memanfaatkan fasilitas tersebut, tentu sayang rasanya jika kita punya barang bagus tapi hanya digelestakan begitu saja. Buku ini akan menjelaskan konsep, langkah praktis, bahkan tips dan trik yang berguna dalam membedah sistem keamanan Windows 8. Perlu Anda ketahui juga, bahwa dalam setiap bab dalam buku ini akan dipaparkan sistem keamanannya.

Namun, perlu Anda ketahui untuk pengamanan yang lebih ketat kita harus bisa mengkombinasikannya. Sangat disarankan, Anda membaca buku ini secara berurutan walaupun dalam beberapa kasus Anda bisa melompatinya.

Saya tidak ingin berlama-lama dalam bab Pendahuluan ini. Akan lebih baik, jika Anda meneruskan sendiri membedah *Sistem Keamanan Windows 8 & Windows 8.1* dengan tangan Anda sendiri.

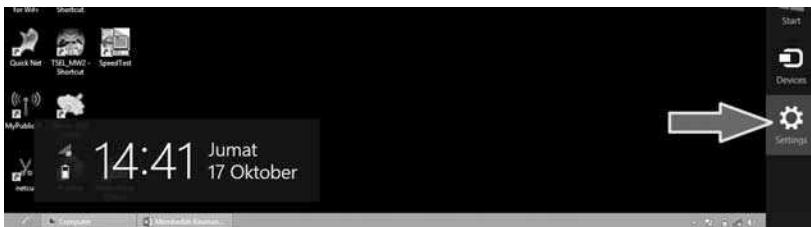
2 MENGELOLA USER ACCOUNTS

Sebagai sistem pengamanan yang pertama dan umumnya pada Windows adalah *user accounts*. Hal ini menjadi pembahasan pertama kali dalam buku ini, karena sewaktu melakukan instalasi maka pembuatan sebuah *user accounts* adalah hal yang mutlak dilakukan.

Untuk melihat *account* yang terdapat dalam Windows 8, adalah melalui Control Panel. Perlu saya jelaskan terlebih dahulu, cara membuka Control Panel pada Windows 8, supaya untuk bab-bab berikutnya yang berhubungan dengan Control Panel saya tidak perlu lagi menjelaskan cara membuka Control Panel.

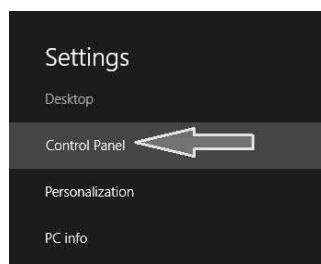
Berikut adalah cara membuka Control Panel pada Windows 8:

1. Arahkan mouse pada sudut kanan atas layar monitor Anda maka akan tampil beberapa menu.
2. Dari menu yang tampil tersebut klik pada bagian **Settings**.



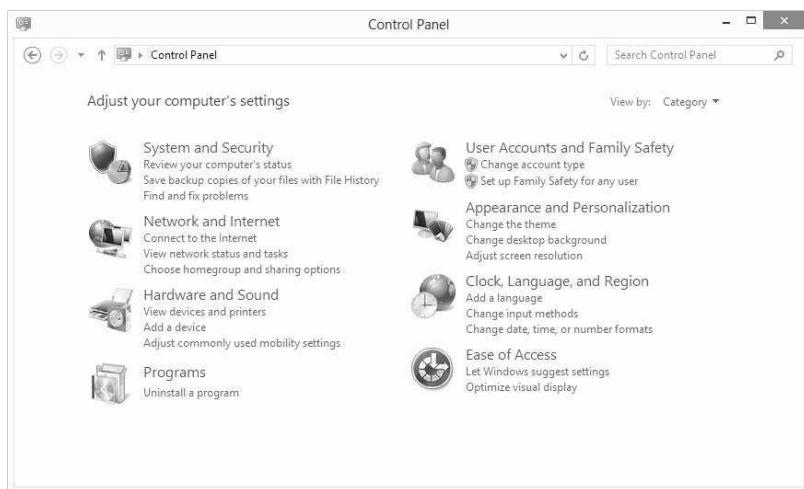
Gambar 2.1 Pilihan Settings

3. Dari tampilan berikutnya, klik pilihan **Control Panel**.



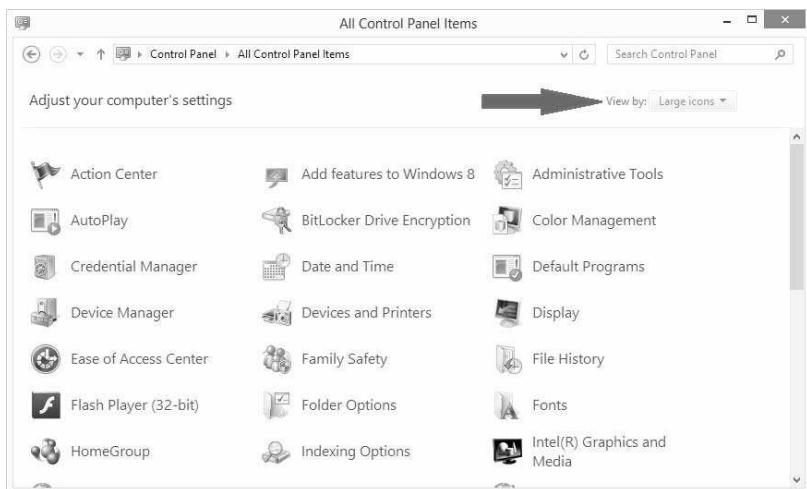
Gambar 2.2 Memilih Control Panel

4. Jika Anda belum pernah mengotak-atik Control Panel maka secara default tampilannya adalah dalam bentuk pengelompokan yang disebut dengan *Category*.



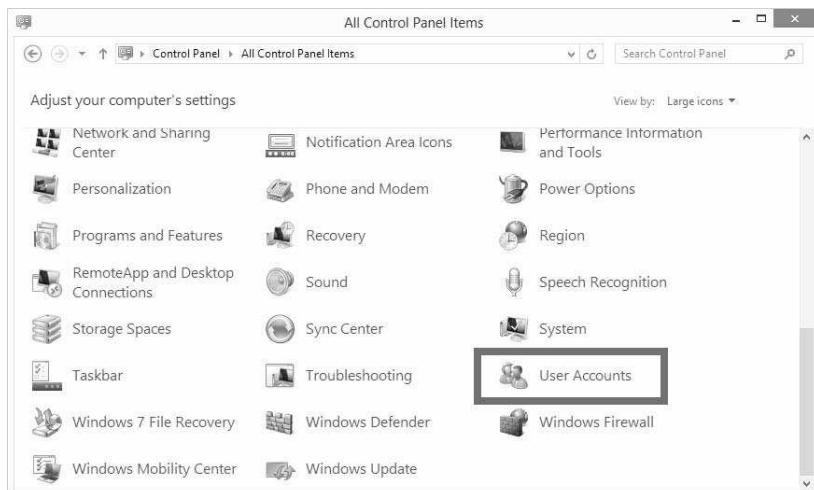
Gambar 2.3 Control Panel

5. Supaya memudahkan kita dalam menyamakan persepsi cara menjalankan Control Panel nantinya. Maka gantilah tampilannya dengan mengubah pilihan *View by* menjadi **Large Icons** yang berada pada bagian kanan atas halaman Control Panel. Hal ini bertujuan supaya semua fitur yang ada bisa terlihat.



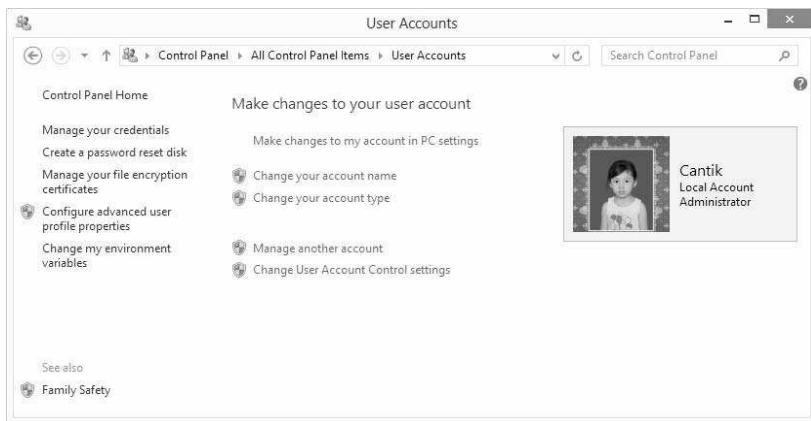
Gambar 2.4 Large Icons

Baiklah, sekarang kita sudah bisa menampilkan semua fasilitas dalam Control Panel. Mari kita lanjutkan kembali pembahasan kita mengenai *User Accounts*. Untuk mengetahui nama user yang terdapat dalam Windows 8, klik pada pilihan **User Accounts** dalam Control Panel.



Gambar 2.5 Memilih *User Accounts*

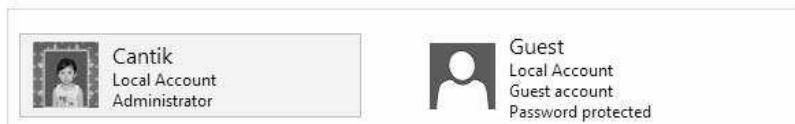
Secara default akan tampil *username* yang aktif dan sedang digunakan oleh Windows atau disebut pula *current user*.



Gambar 2.6 User Accounts

Untuk mengetahui account lainnya yang terdapat dalam Windows 8, klik pada link **Manage another account**. Dari gambar di bawah ini terlihat dua buah account yang terdapat dalam komputer saya, yaitu account *Administrator* dengan nama “Cantik”, dan juga sebuah account *Guest*.

Choose the user you would like to change



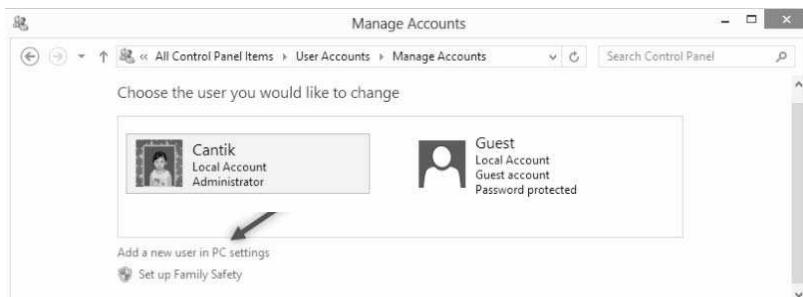
Gambar 2.7 Account yang tersedia

Dari informasi yang ditampilkan kita juga bisa mengetahui bahwa account Cantik tidak menggunakan password. Sedangkan account Guest menggunakan password. Hal ini diketahui dari pesan yang ditampilkan berupa *Password Protected*.

Setelah mengetahui account apa saja yang terdapat dalam Windows. Berikutnya kita akan membahas beberapa pengaturan lainnya yang bisa Anda terapkan pada sebuah account.

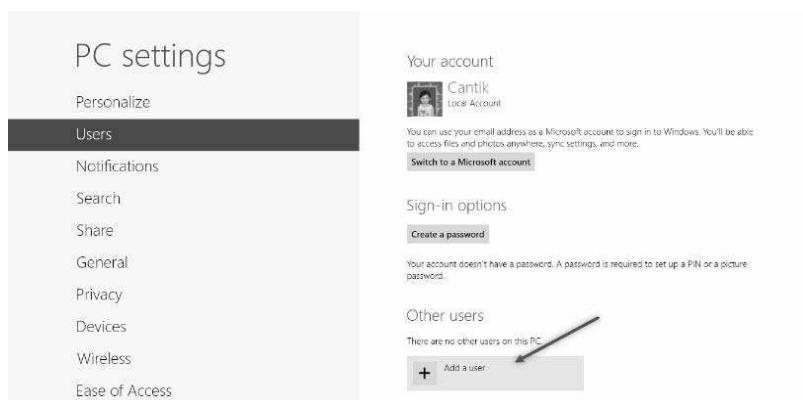
2.1 Menambah Account

Apabila Anda ingin menambahkan sebuah account dalam Windows. Dari dalam halaman yang sama pada bagian nama-nama *account* tersebut, perhatikan pada bagian bawah, klik pada link **Add a new user in PC Settings.**



Gambar 2.8 Memilih Add a new user in PC settings

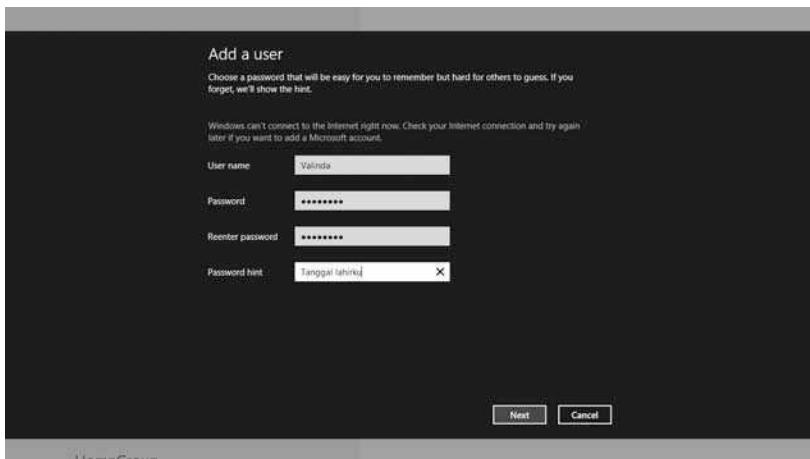
Maka tampilan Windows akan berubah, lalu klik pada bagian **Add a user.**



Gambar 2.9 Memilih Add a user

Dari halaman *Add a user*, masukkanlah nama account yang Anda inginkan pada bagian *User name*. Sebaiknya pula Anda mengisi bagian

password, supaya orang yang tidak berhak tidak dapat mengakses account tersebut. Sedangkan fungsi dari *Password hint* adalah untuk memberitahukan kata kunci apa password yang Anda gunakan. Setelah selesai, klik tombol **Next**.



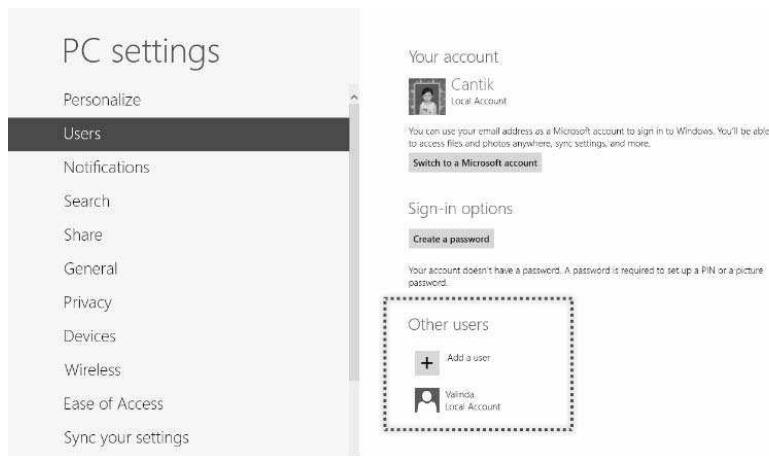
Gambar 2.10 Membuat user

Selanjutnya akan tampil informasi nama account yang baru saja Anda buat. Apabila account tersebut akan digunakan oleh anak Anda, maka sangat disarankan untuk memberikan tanda centang pada bagian *Is this a child's account? Turn on Family Safety to get reports of their PC use.* Fungsinya adalah untuk memonitor pemakaian komputer oleh anak atau anggota keluarga Anda yang lainnya. Setelah selesai, klik tombol **Finish**.



Gambar 2.11 Account baru

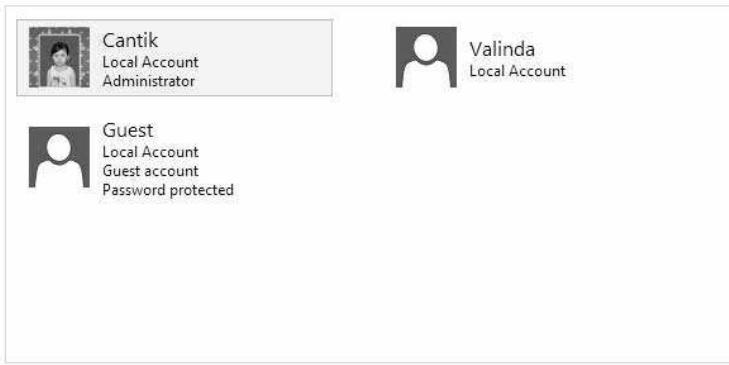
Sekembalinya Anda pada halaman sebelumnya maka nama account yang baru akan tampil.



Gambar 2.12 User baru selesai dibuat

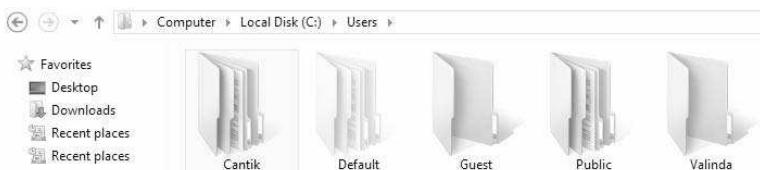
Selain itu, pada halaman *Manage Accounts* juga akan tampil nama account yang baru saja Anda buat.

Choose the user you would like to change



Gambar 2.13 Daftar nama account

Untuk setiap account yang dibuat dalam Windows 8 secara otomatis akan dibuatkan sebuah folder profil tersendiri yang berfungsi sebagai lokasi penyimpanan data masing-masing, tampilan desktop yang berbeda dan sebagainya. Letak folder profil tersebut disimpan dalam “C:\Users”, di dalamnya terdapat subfolder yang berisikan folder sesuai dengan nama-nama account yang ada dalam komputer Anda.

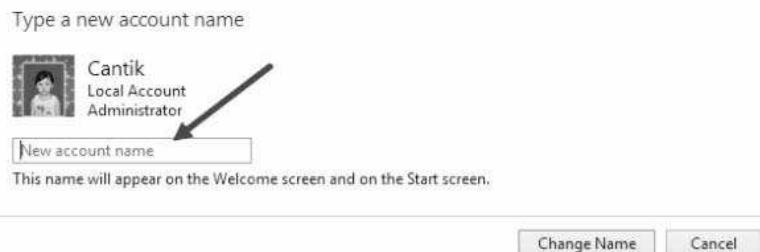


Gambar 2.14 Folder user

2.2 Mengubah Nama Account

Entah pikiran apa yang merasuki Anda, lalu tiba-tiba ingin mengganti nama account yang pernah Anda buat. Untuk mengubah nama account, pada halaman awal *User Accounts* klik link **Change your account name**.

Selanjutnya, dari bagian *Type a new account name*, ketiklah nama yang Anda inginkan pada tempat yang bertuliskan *New account name*. Sebagai contoh di sini saya akan menggunakan nama WindowsKu. Setelah selesai, klik tombol **Change Name**.



Gambar 2.15 Memasukkan nama account baru

Sekembalinya Anda pada halaman sebelumnya maka nama Anda yang baru Anda buat tersebut langsung diaktifkan.



Gambar 2.16 Nama account berubah

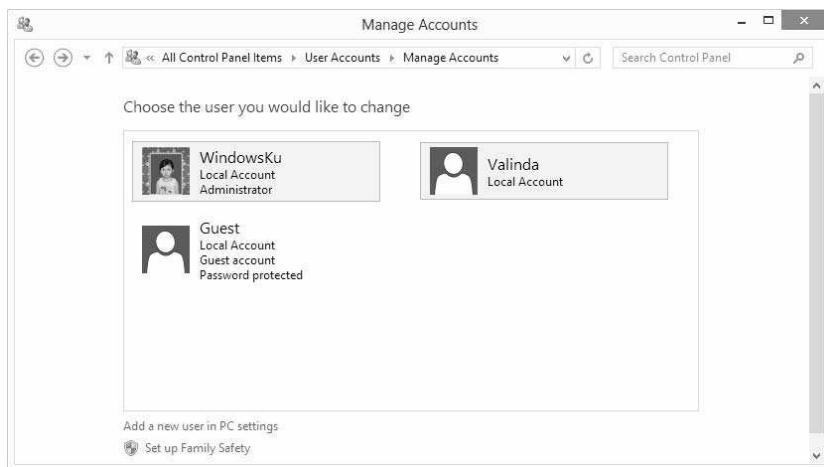
2.3 Mengubah Status Account

Perlu Anda ketahui bahwa dalam Windows 8 terdapat dua jenis account, yaitu:

- Account Standard yang digunakan apabila Anda tidak ingin mengubah berbagai setting dalam Windows 8.
- Account Administrator adalah account yang bisa mengontrol sepenuhnya sistem operasi Windows 8, seperti halnya mengubah setting Windows termasuk mengakses semua file dan program yang terdapat dalam komputer.

Andaikata Anda tidak ingin orang lain yang meminjam komputer Anda bisa mengakses sistem dan data dalam komputer Anda maka buatkanlah account standard. Sebab apabila account standard akan melakukan instalasi program atau mengubah sistem keamanan maka diharuskan untuk memasukkan password administrator.

Supaya bisa mengubah account, maka status Anda dalam Windows haruslah sebagai administrator. Sebagai contoh di sini, kita akan mengubah status sebuah account, klik kembali link **Manage another account**. Dari beberapa nama account yang terdapat dalam komputer, klik pada account yang ingin Anda ganti statusnya. Sekarang saya akan mengganti status account yang bernama Valinda yang telah kita buat sebelumnya. Klik pada nama account tersebut.



Gambar 2.17 Memilih account

Setelah Anda mengklik account, lanjutkan dengan mengklik **Change the account type**.

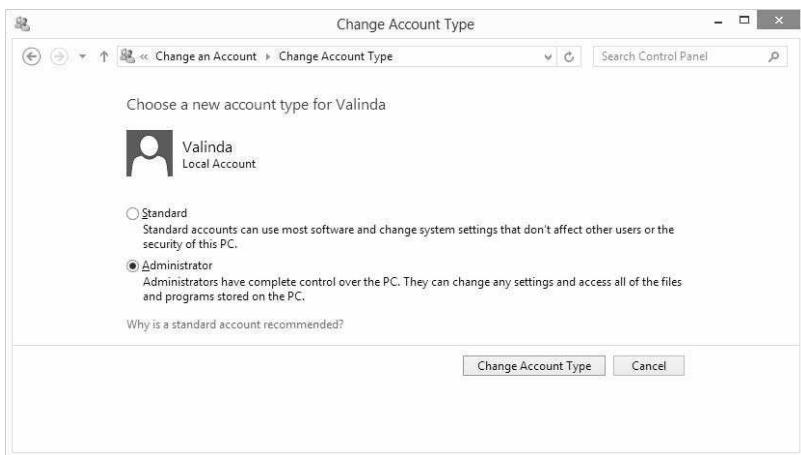
Make changes to Valinda's account

Change the account name.
Create a password
Set up Family Safety
Change the account type
Delete the account
Manage another account



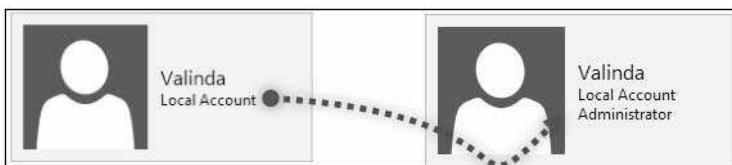
Gambar 2.18 Mengubah jenis account

Berikutnya, pilih salah satu pilihan yang disediakan, apakah Anda ingin mengganti status sebuah account menjadi *Standard* atau menjadi *Administrator*. Setelah selesai, klik tombol **Change Account Type**.



Gambar 2.19 Memilih Administrator

Jika Anda perhatikan pada nama account tersebut yang semula *Standard* kini telah berubah menjadi *Administrator*.



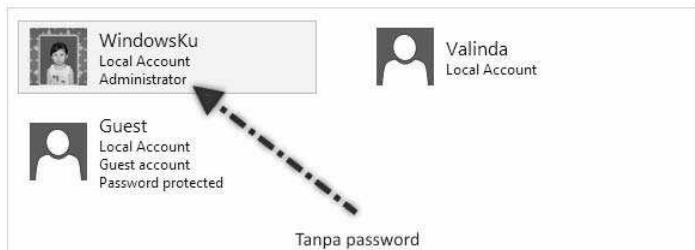
Gambar 2.20 Status account berubah

2.4 Memasang Password

Password adalah fitur keamanan yang paling penting dan tidak boleh diabaikan. Oleh karena itu, apabila account Anda belum terpasang password, sudah waktunya Anda memasang password tersebut. Terutama sekali dalam sebuah komputer yang terdiri atas beberapa account. Hal ini bertujuan untuk mencegah orang lain mengobok-obok account lainnya.

Untuk memasang ataupun mengubah password account, setelah Anda berada pada halaman *Choose the user you would like to change*, klik pada salah satu account yang akan dipasang password.

Choose the user you would like to change



Gambar 2.21 Memilih account

Dari tampilan berikutnya, klik pada menu **Create a password**

Make changes to WindowsKu's account

- Change the account name
- Create a password** (highlighted with a solid arrow pointing to it)
- Set up Family Safety
- Change the account type
- Manage another account



Gambar 2.22 Memilih Create a password

Sekarang isilah password yang Anda inginkan pada tempat yang telah disediakan. Ulangi sekali lagi pengisian passwordnya pada bagian *Confirm new password*.

Untuk *Type a password hint*, sebenarnya lebih saya sarankan untuk tidak diisi. Karena kalau Anda mengisinya maka seseorang bisa dengan mudah mencoba menebak password yang Anda gunakan. Misalnya Anda menggunakan password dengan nama artis favorit, lalu pada bagian *password hint* Anda isi dengan "artis favoritku", tentu saja orang lain bisa mengira-ngira password milik Anda. Atau Anda bisa memanfaatkan fasilitas *hint* untuk mengelabui orang lain, misalnya password yang Anda gunakan adalah nama artis favorit, lalu pada bagian *password hint* bisa Anda isi dengan "Makanan favoritku".

Setelah semua hal di atas selesai dilakukan klik tombol **Create password**.

Create a password for WindowsKu's account



WindowsKu
Local Account
Administrator

You are creating a password for WindowsKu.

If you do this, WindowsKu will lose all EFS-encrypted files, personal certificates and stored passwords for Web sites or network resources.

If the password contains capital letters, they must be typed the same way every time.

The password hint will be visible to everyone who uses this computer.

Gambar 2.23 Memasukkan password

Jika Anda perhatikan pada status account tersebut, telah berubah dengan adanya pesan *Password protected*.

Make changes to WindowsKu's account

Change the account name

Change the password

Set up Family Safety

Change the account type

Manage another account



Gambar 2.24 Account sudah di-password

2.5 Mengganti Password

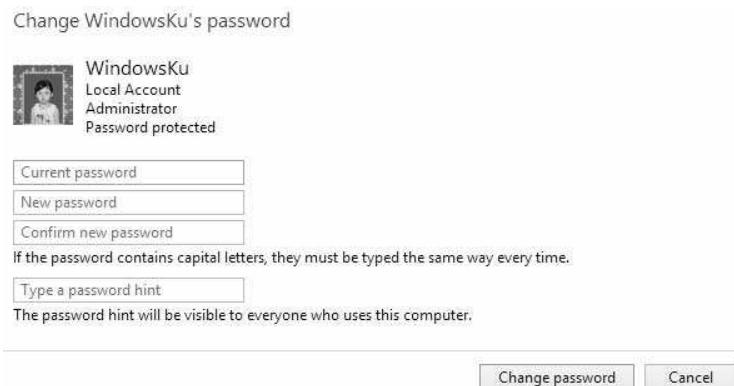
Demi keamanan komputer maka disarankan juga untuk mengganti password secara berkala. Tujuannya, supaya orang lain tidak bisa mengintip password Anda. Fasilitas ini hanya akan aktif apabila sebelumnya Anda telah memasang password terlebih dahulu.

Untuk mengganti password, pertama-tama carilah account yang akan Anda ganti password-nya. Dilanjutkan dengan mengklik link **Change the password**.



Gambar 2.25 Memilih Change the password

Dari tampilan berikutnya, pada bagian *Current password* masukkanlah password Anda yang terdahulu. Sedangkan pada bagian *New password* dan *Confirm new password*, isikan dengan password yang baru. Jika Anda tidak ingin memakai password maka kosongkanlah pada kedua bagian tersebut dan tindakan ini tidak disarankan. Terakhir klik tombol **Change password**.

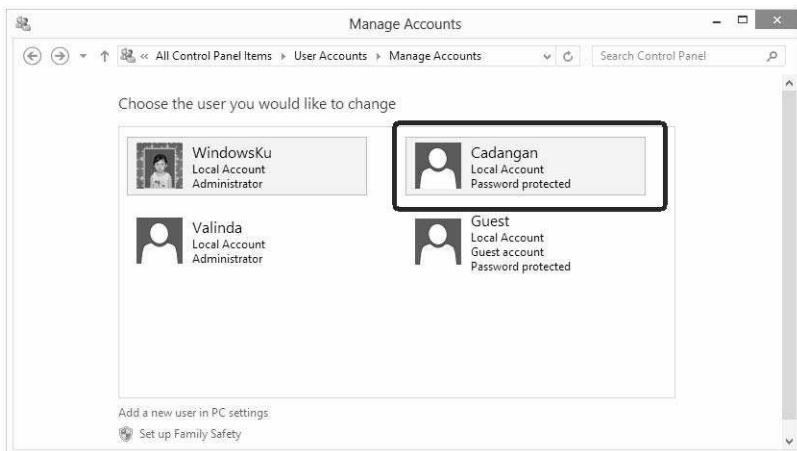


Gambar 2.26 Memasukkan password baru

2.6 Menghapus Account

Apabila dalam komputer Anda terdapat cukup banyak account sehingga Anda merasa ada account yang perlu dihapus.

Masih dari halaman *Manage Account*, klik pada salah satu account yang akan Anda hapus tersebut. Sebagai contoh di sini saya telah membuat sebuah account yang bernama Cadangan. Klik pada nama account tersebut.



Gambar 2.27 Memilih Account Cadangan

Dari tampilan berikutnya, klik pada link **Delete the account**.



Gambar 2.28 Klik Delete the account

Selanjutnya akan tampil pesan pertanyaan yang menanyakan, apakah Anda ingin menghapus file milik account Cadangan, atau membiarkan file-nya tetap berada dalam komputer.

- Jika Anda ingin menghapus file yang terdapat dalam account Cadangan, klik tombol *Delete Files*.

- Sebaliknya, apabila Anda tidak ingin menghapus file-file milik account Cadangan, klik tombol **Keep Files**.

Apabila Anda merasa tidak memerlukan lagi account tersebut maka pilihlah **Delete Files**.

Do you want to keep Cadangan's files?

Before you delete Cadangan's account, Windows can automatically save the contents of Cadangan's desktop and Documents, Favorites, Music, Pictures and Videos folders to a new folder called 'Cadangan' on your desktop. However, Windows cannot save Cadangan's e-mail messages and other settings.

Gambar 2.29 Pilihan penghapusan

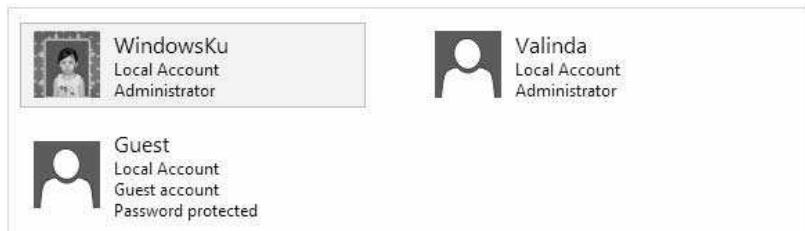
Berikutnya akan tampil pertanyaan konfirmasi, apakah Anda yakin akan menghapus account yang Anda pilih? Jika iya, klik tombol **Delete Account**.

Are you sure you want to delete Cadangan's account?

Windows will delete all of Cadangan's files, and then delete Cadangan's account.

Gambar 2.30 Konfirmasi menghapus account

Sekembalinya pada halaman nama-nama account maka account yang bernama Cadangan sudah tidak tampil lagi.



Gambar 2.31 Account Cadangan telah dihapus

Sekarang mari kita tengok skenario lainnya, apabila sewaktu menghapus sebuah account dan Anda memilih opsi **Keep Files**. Maka setelah account tersebut terhapus pada desktop akan muncul sebuah folder baru sesuai dengan nama komputer Anda. Dan di dalam folder tersebut terdapat sebuah folder lagi yang bernama sesuai dengan account yang telah dihapus. Dalam folder itulah keberadaan file-file milik account yang dihapus tersebut.

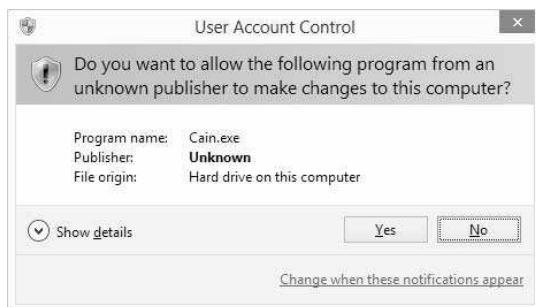
Gambar di bawah ini memperlihatkan folder dengan nama Valinda yang account-nya telah saya hapus.



Gambar 2.32 Folder account yang dihapus

2.7 User Account Control

Sebelum menjelaskan bagian ini, terlebih dahulu saya ingin menampilkan sebuah kotak dialog yang sering tampil pada Windows 8. Kotak dialog ini bernama *User Account Control*. Pernahkah Anda melihat kotak dialog seperti gambar di bawah ini? Atau yang semirip dengannya?



Gambar 2.33 *User Account Control*

Saya rasa Anda sudah sering melihatnya. Terutama untuk program yang memiliki tanda berupa ikon tameng. Hal ini menunjukkan bahwa program tersebut tidak dikenal *publisher*-nya atau memerlukan account administrator untuk dapat menggunakannya. Program-program yang seperti itu akan mengubah sistem sehingga perlu dilakukan konfirmasi terlebih dahulu sebelum program tersebut di-eksekusi. Umumnya hal ini ditandai dengan adanya ikon tameng berwarna kuning pada sebuah file aplikasi maupun *shortcut*-nya.



Gambar 2.34 *Penanda program yang memerlukan account administrator atau akan mengubah sistem*

Perlu Anda ketahui bahwa *User Account Control* adalah salah satu fitur pengamanan yang mulai terdapat pada Windows Vista. Tujuannya adalah menampilkan kotak dialog yang menanyakan *privileges* untuk program tertentu, terutama terhadap program yang akan mengubah sistem sewaktu berjalan atau sewaktu proses instalasi.

Cara kerja dari *User Account Control* ini adalah untuk memaksa kita sewaktu menggunakan Windows berperan sebagai account standard biasa. Walaupun kita login dengan account administrator. Mungkin ada

sebagian pembaca yang bingung, kok kita login dengan account administrator tapi dipaksa berberan sebagai account standard.

Untuk mempermudah pemahaman, mari kita ulang kembali bahwa pada Windows 8 terdapat dua jenis account, yaitu standard dan administrator. Account yang diizinkan untuk mengubah setting sistem operasi hanyalah account administrator, sedangkan account standard tidak diperkenankan untuk mengubah sistem. Oleh karena itu, sewaktu account standard akan menjalankan program yang bisa mengubah sistem akan muncul kotak dialog yang meminta Anda untuk memasukkan password administrator.

Misalnya, ketika kita akan menjalankan Command Prompt dengan status Administrator (*Run as administrator*). Apabila kita login dengan account standard maka akan tampil kotak dialog *User Account Control* yang meminta Anda untuk memasukkan password account administrator-nya.



Gambar 2.35 Permintaan password

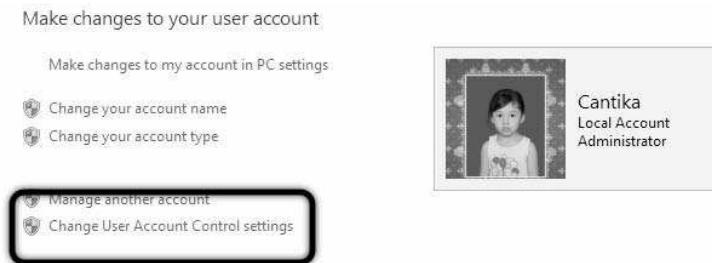
Sekarang, apabila kita akan menjalankan *Command Prompt as Administrator*, dan kita login menggunakan account administrator. Maka yang tampil adalah kotak dialog *User Account Control*, yang berisikan pertanyaan apakah Anda akan menjalankan program tersebut atau tidak? Oleh karena kita sudah login sebagai administrator maka password tidak diminta lagi, melainkan hanya pesan konfirmasi.



Gambar 2.36 Kotak dialog UAC

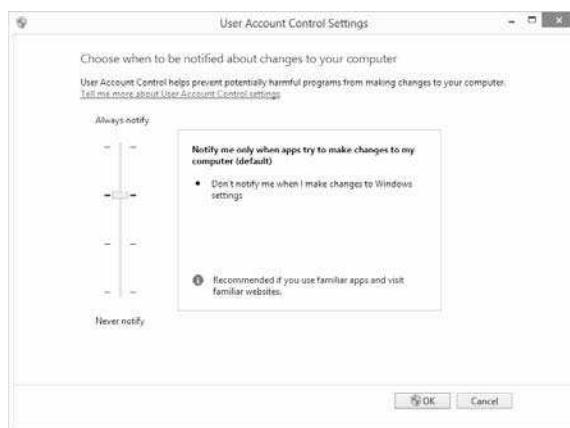
Nah, dari kedua gambaran di atas, terlihat baik kita login sebagai account standard maupun sebagai account administrator. Keduanya akan tetap meminta kita untuk menjalankan aplikasi tertentu. Terutama aplikasi yang bisa mengubah sistem. Dengan demikian hal ini menunjukkan bahwa sebenarnya posisi kita sewaktu menggunakan Windows dipaksa menjadi account standard. Tujuannya, tentu saja supaya tidak sembarang program bisa berjalan atau aktif seenaknya untuk mengubah sistem Windows yang efeknya bisa merusak. Saya harap, Anda bisa memahami penjelasan *User Account Control* ini.

Tidak semua orang suka dipaksa menjalani perannya sebagai account standard ini. Jadi kita bisa menyettingnya. Untuk mengatur *User Account Control* tersebut, dalam halaman *User Accounts*, klik pada **Change User Account Control Settings**.



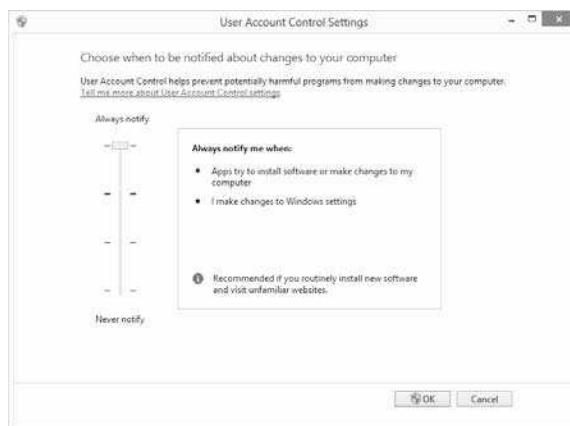
Gambar 2.37 Memilih Change User Account settings

Secara default, Anda dalam posisi tingkat keamanan level 3, yang berarti Anda akan diperingatkan setiap kali ada program yang akan mengubah sistem berjalan.



Gambar 2.38 *User Account Control Settings*

Supaya menjadi lebih aman, Anda bisa menggeser *slider* pada posisi yang paling atas. Pilihan ini akan menerapkan setiap kali ada proses penginstalan atau adanya perubahan terhadap sistem akan selalu menampilkan kotak dialog notifikasi. Setelah selesai, klik tombol **OK**.



Gambar 2.39 *Mengubah User Account Control Settings*

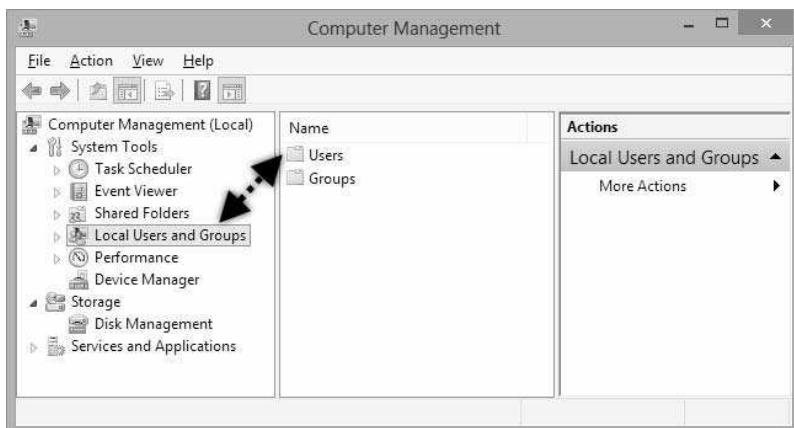
Sebaliknya, apabila Anda merasa dengan tampilnya kotak dialog konfirmasi tersebut malah mengganggu. Anda juga diperkenankan untuk menonaktifkannya, dengan cara menggeser *slider* ke bagian yang paling bawah (*Never notify*). Namun, perlu Anda ketahui, jika Anda memilih opsi ini maka apabila ada program yang diam-diam menginstall dirinya atau melakukan perubahan seperti oleh virus menjadi tidak terdeteksi lagi oleh Windows. Jadi, aturlah dengan bijak.

2.8 Tips

Untuk keamanan Anda dalam menggunakan komputer, sebaiknya Anda membuat beberapa buah account apabila komputer Anda digunakan lebih dari satu orang. Dan buatlah account untuk orang lain menggunakan status Standard. Cukup hanya account Anda sendiri saja yang memegang status administrator.

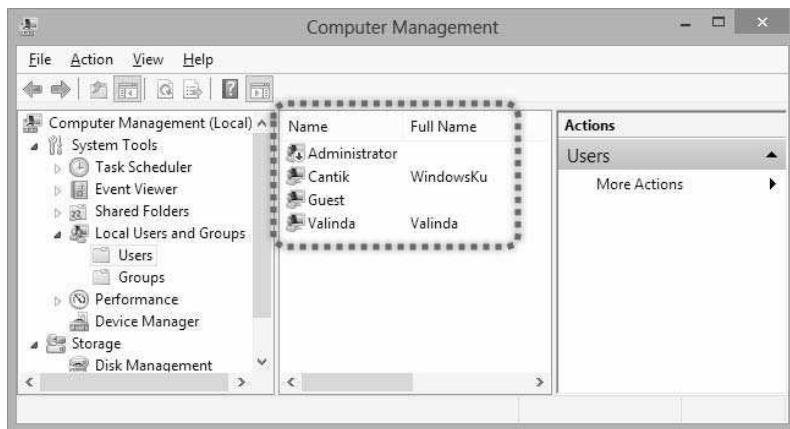
Informasi mengenai account apa saja yang terdapat dalam Windows juga bisa Anda lihat dalam fitu *Computer Management*. Dalam Control Panel bukalah **Administrative Tools**, kemudian jalankan **Computer Management**.

Selanjutnya, dalam jendela kerja *Computer Management*, pada panel sebelah kiri klik pada **Local Users and Groups** hasilnya pada panel sebelah kanan akan tampil dua buah folder, yaitu *Users* dan *Groups*.



Gambar 2.40 *Computer Management*

Klik folder *Users* untuk mengetahui nama-nama account yang terdapat dalam komputer.



Gambar 2.41 Nama-nama user

Jika Anda perhatikan terdapat sebuah account lain yang bernama *Administrator*. Account tersebut adalah account *built-in* yang dibuat oleh Windows.

3

MICROSOFT ACCOUNT

Berbeda dengan Windows versi sebelumnya, pada Windows 8 terdapat dua cara untuk bisa login ke Windows. Yang pertama adalah yang disebut dengan *Local Account* yang telah kita bahas dalam bab sebelumnya. Sedangkan metode yang kedua adalah menggunakan *Microsoft Account*.

Sebenarnya Microsoft Account adalah account yang umumnya dibuat pada website milik Microsoft, seperti Hotmail, Windows Live atau Outlook. Semua layanan tersebut bisa Anda dapatkan secara gratis dari website-nya milik Microsoft. Sedangkan Local Account Anda bisa membuatnya pada komputer tanpa perlu terhubung ke internet.

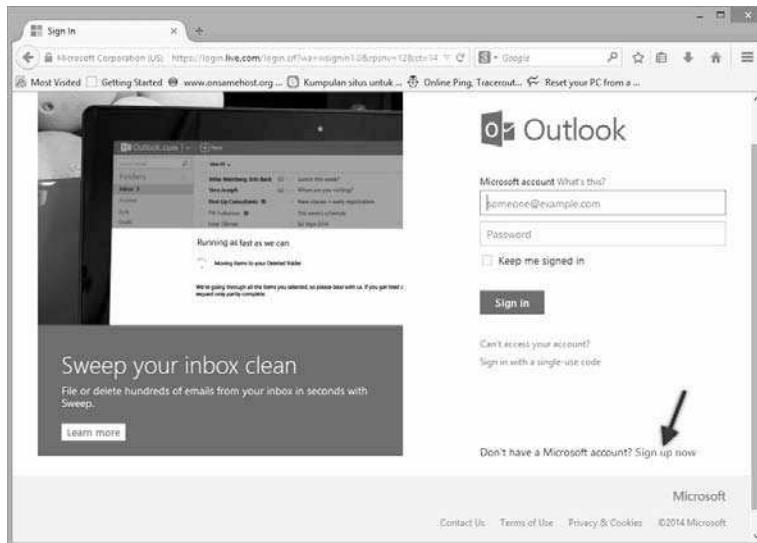
Dengan memiliki Microsoft Account maka Anda memiliki keleluasaan untuk mendownload berbagai aplikasi yang disediakan di Windows Store yang beralamatkan di <http://www.microsoftstore.com>. Selain itu dengan memiliki Microsoft Account maka kita memiliki akses ke OneDrive untuk melakukan sinkronisasi (back-up data), serta bisa memanfaatkan tampilan metro. Jadi, boleh dibilang Microsoft Account adalah layanan terpadu dari Microsoft di mana dengan satu buah account saja, Anda bisa mengakses banyak hal lainnya. Seperti Messenger, Xbox Live, Windows Phone, dan layanan Microsoft lainnya.

3.1 Mendaftar Account

Sebelum Anda dapat menggunakan Microsoft Account maka Anda harus mendaftar sebuah account terlebih dahulu, dan pastikan Anda sudah terhubung ke internet.

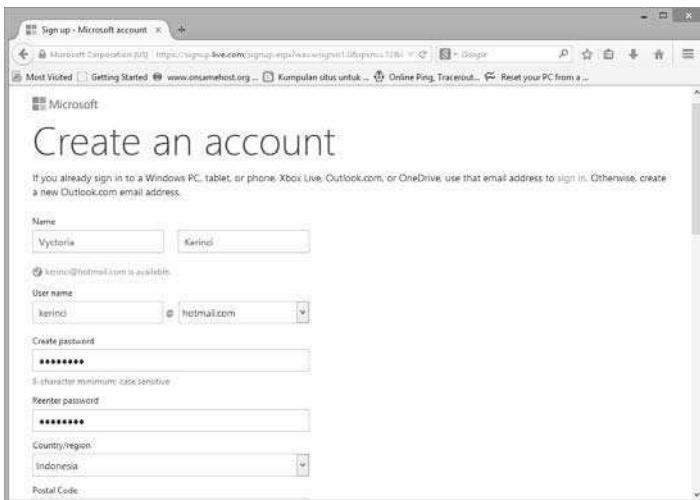
Jika Anda sudah pernah mendaftar sebuah account di Windows Live ID atau Hotmail maka bagian ini bisa Anda lewati. Bagi Anda yang belum memiliki account di Microsoft ikuti langkah berikut untuk mendapatkannya:

1. Bukalah browser Anda dan kunjungi live.com, kemudian klik link **Sign up now**.



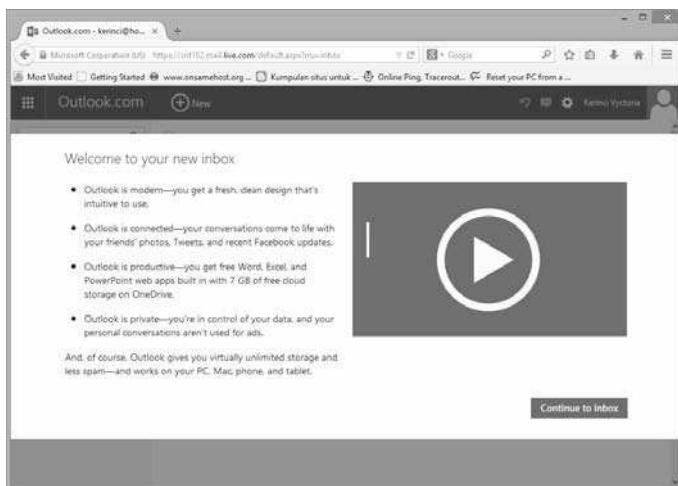
Gambar 3.1 *Live.com*

2. Dari halaman pengisian formulir, masukkanlah data-data yang diminta secara lengkap, dan klik tombol **Create Account** yang berada pada bagian paling bawah.



Gambar 3.2 Formulir pengisian biodata

3. Apabila semuanya berjalan lancar maka Anda bisa langsung ke inbox dengan mengklik tombol **Continue to Inbox**. Di dalamnya, Anda dapat melihat sebuah email ucapan selamat datang.



Gambar 3.3 Account berhasil dibuat

Setelah Anda memiliki sebuah account, sekarang Anda bisa menggunakanya sebagai Microsoft Account pada Windows 8. Perlu Anda ketahui juga bahwa Microsoft Account mengharuskan Anda login ke account Microsoft misalnya Hotmail minimal setiap 270 hari sekali. Apabila Anda tidak pernah login menggunakan account tersebut, maka account Anda akan dihapus secara otomatis.

Untuk mendaftar sebuah account Microsoft, caranya tidak hanya dengan membuka website seperti yang telah saya jelaskan sebelumnya. Anda juga bisa mendaftarkan sebuah account langsung dari komputer pada halaman PC Settings. Oleh karena langkah yang dilakukan tetaplah sama, dan yang membedakan hanyalah tampilannya. Jadi, cukup saya jelaskan satu cara saja, daripada cuma nambah-nambah halaman untuk hal yang tidak begitu penting.

3.2 Beralih ke Microsoft Account

Jika Anda berminat untuk beralih ke Microsoft Account, ikuti langkah berikut ini. Namun satu hal yang pasti, Anda sudah harus terhubung ke internet untuk dapat melakukannya. Selain itu, bagi Anda yang masih belum memiliki account, buatlah sebuah account di live.com, seperti yang telah dijelaskan di atas.

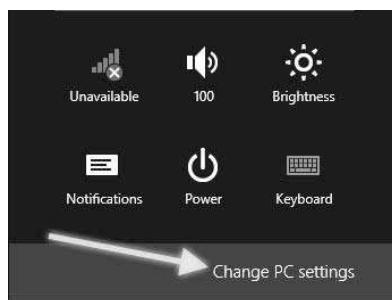
Untuk beralih menggunakan Microsoft Account Anda harus masuk ke dalam halaman *PC Settings* terlebih dahulu, untuk lebih jelasnya ikuti langkah berikut ini:

1. Setelah Anda login dalam Windows, arahkan mouse pada sudut kanan atas maka akan tampil beberapa menu. Dari menu yang muncul, klik **Settings**.



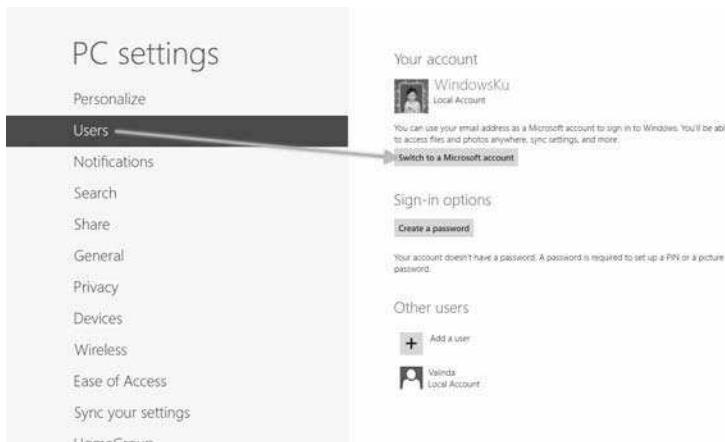
Gambar 3.4 Memilih *Settings*

2. Kemudian tampilan menu tersebut akan berubah. Dari beberapa pilihan *Settings* yang tersedia, klik **Change PC Settings** yang berada pada bagian paling bawah.



Gambar 3.5 Klik Change PC settings

3. Dalam halaman *PC settings*, klik **Users**. Sedangkan isinya di sebelah kanan klik tombol **Switch to a Microsoft Account**.



Gambar 3.6 Switch to a Microsoft Account

4. Selanjutnya, masukkanlah alamat email yang telah Anda buat pada subbab sebelumnya kemudian klik **Next**.

Sign in with a Microsoft account

Use your favorite email address to sign in to Windows. If you already use an email address to sign in to PCs running Windows, enter it here.

Email address

Gambar 3.7 Memasukkan email

5. Selanjutnya masukkanlah password email Anda dan klik **Next**.

④ Sign in to your Microsoft account

Sign in to easily get your online email, photos, files, and settings (like browser history and favorites) on all your devices. You can manage your synced settings at any time.

kerinci@hotmail.com

.....



Gambar 3.8 Memasukkan password

6. Sekarang Anda telah siap untuk masuk menggunakan Microsoft Account, klik **Finish**.

Sign in with a Microsoft account



Vyctoria Kerinci

kerinci@hotmail.com

You're almost done changing your account. Next time you sign in to Windows, use your Microsoft account and password.

Finish

Cancel

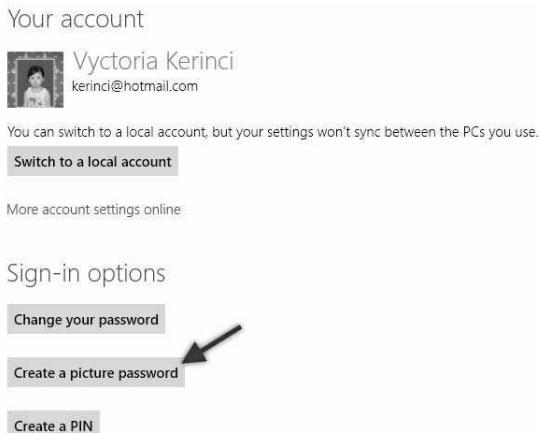
Gambar 3.9 Proses selesai

Sekembalinya Anda pada halaman PC Setting maka Anda sudah siap menggunakan Microsoft Account untuk login.

3.3 Picture Password

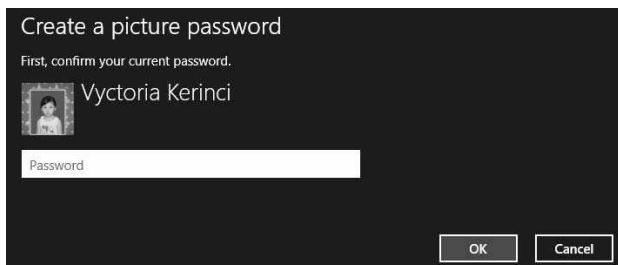
Salah satu kelebihan dari penggunaan Microsoft Account adalah kita bisa membuat password dari gambar atau PIN. Sebagai contoh saya akan membuat password berupa gambar atau *image*.

Kembali pada halaman PC Setting pada bagian *Users*, klik pada **Create a picture password**.



Gambar 3.10 Create a picture password

Pertama-tama Anda harus mengkonfirmasi dengan memasukkan password Microsoft Account milik Anda. Setelah Anda memasukkan password, klik **OK**.



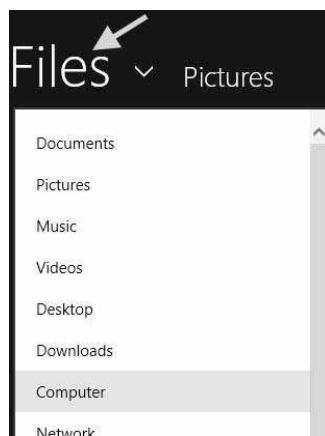
Gambar 3.11 Memasukkan password

Dari gambar yang muncul, *drag* atau buatlah pola gambar yang akan Anda jadikan password. Jika Anda ingin mengganti gambar yang tersedia, klik tombol *Choose picture* yang berada di panel sebelah kiri.



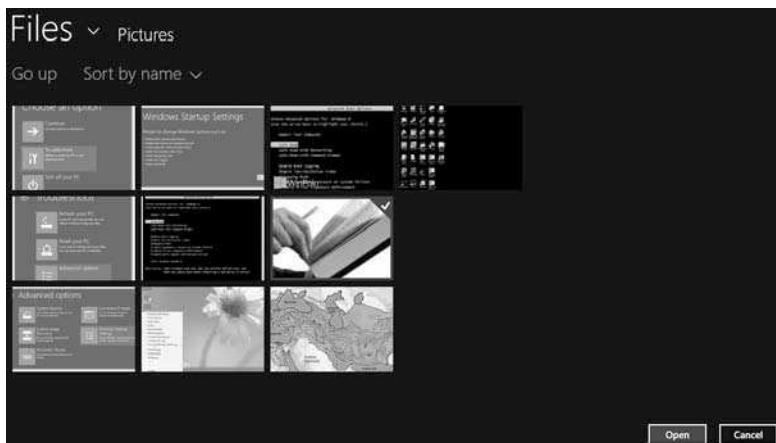
Gambar 3.12 Perhatikan contoh membuat gerakan/pola password

Selanjutnya carilah gambar yang akan Anda gunakan sebagai password. Jika Anda ingin mencari gambar pada lokasi lainnya, klik pada bagian **Files** lalu carilah gambar yang Anda inginkan.



Gambar 3.13 Menu File

Apabila Anda sudah menemukan gambar yang sesuai, klik pada gambar tersebut dan klik tombol **Open**.



Gambar 3.14 Memilih gambar

Gambar yang dipilih akan tampil, jika Anda setuju untuk menggunakan gambar tersebut sebagai password, klik tombol **Use this picture**.



Gambar 3.15 Gambar siap digunakan

Berikutnya buatlah gerakan untuk digunakan sebagai password Anda. Anda bisa membuat gerakan melingkar, garis lurus dan sebagainya. Yang penting Anda ingat dengan gerakan tersebut. Sebagai contoh di bawah ini, saya membuat garis lurus saja. Lakukan gerakan tersebut sebanyak tiga kali. Anda juga bisa membuat tiga gerakan yang berbeda atau cukup mengklik pada titik-titik tertentu saja.



Gambar 3.16 Membuat gerakan/pola password di gambar

Diikuti dengan mengulangi gerakan yang tadi sebagai konfirmasi. Apabila setelah tiga kali Anda membuat gerakan yang konsisten dengan sebelumnya maka akan muncul tombol **Finish**, klik tombol tersebut.

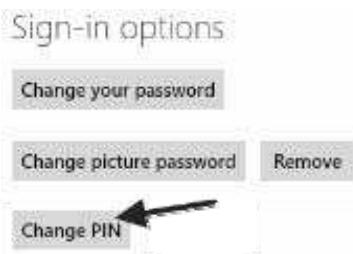


Gambar 3.17 Picture password siap digunakan

Terakhir, sekembalinya Anda pada kotak dialog PC Setting berarti proses pemasangan password gambar telah selesai. Selanjutnya, pada tampilan login Windows akan terdapat pilihan untuk memasukkan password dengan gambar yang Anda pilih. Yang harus Anda lakukan adalah mencocokkan ketiga gerakan yang telah Anda buat sebelumnya sebanyak tiga kali.

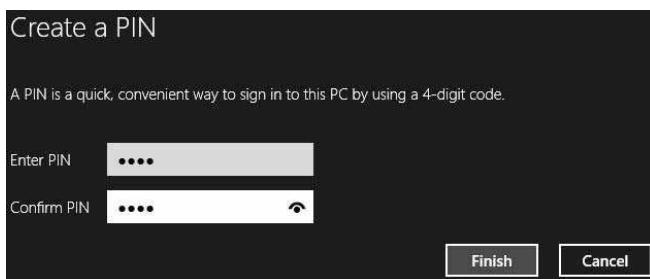
3.4 Menggunakan PIN

Selain menggunakan gambar (*picture*), Anda juga bisa login pada Windows 8 menggunakan PIN. Untuk membuatnya sama pada seperti membuat *picture password* dalam jendela kerja PC Settings pada bagian *Users*, klik pada bagian **Change PIN**.



Gambar 3.18 Change PIN

Dari halaman yang tampil, masukkanlah PIN yang Anda inginkan kemudian klik tombol **Finish**.



Gambar 3.19 Memasukkan PIN

Sekarang Anda telah memiliki beberapa pilihan untuk login ke dalam Windows 8, selain menggunakan password, kini juga telah tersedia *picture password* dan PIN.

3.5 Kembali ke Local Account

Ada kalanya Anda sudah bosan menggunakan Microsoft Account. Perlu Anda ketahui bahwa setiap saat Anda bisa kembali menggunakan Local Account saja. Caranya adalah sebagai berikut:

1. Dalam jendela kerja PC Settings, masuklah pada bagian *Users*. Dari tampilan yang muncul, klik pada tombol **Switch to a local account**.

Your account



Vyctoria Kerinci

kerinci@hotmail.com

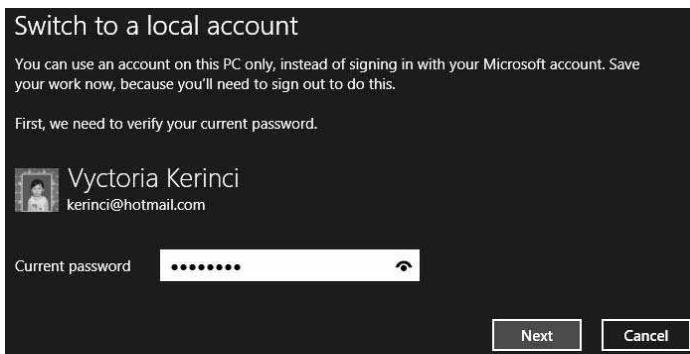
You can switch to a local account, but your settings won't sync between the PCs you use.

Switch to a local account



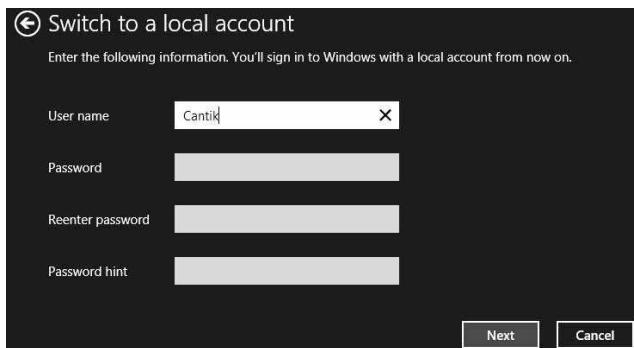
Gambar 3.20 Memilih Switch to a local account

2. Selanjutnya, masukkanlah password yang Anda gunakan dan klik **Next**.



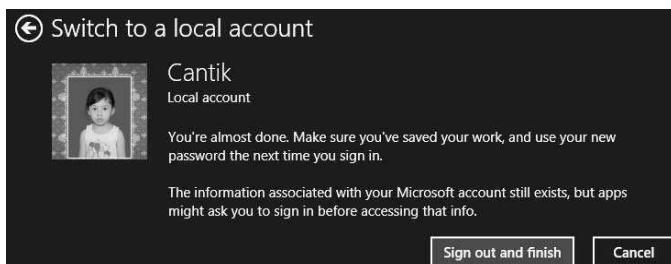
Gambar 3.21 Memasukkan password

3. Setelah itu, isi user dan password Local Account Anda, dan klik **Next**.



Gambar 3.22 Memasukkan username dan password

4. Proses untuk kembali ke Local Account telah siap, klik tombol **Sign out and Finish**.



Gambar 3.23 Proses selesai

Setelah komputer *sign out* maka komputer Anda sudah menggunakan Local Account. Sewaktu Anda kembali ke modus Local Account ini maka fasilitas *Picture Password* dan PIN juga tidak bisa digunakan lagi.

4

PASSWORD RESET DISK

Jika Anda perhatikan pada panel sebelah kiri dalam halaman *User Accounts*, terdapat sebuah menu bertuliskan *Create a password reset disk*. Fasilitas *Reset Disk* tersebut berguna apabila Anda lupa password sehingga tidak bisa melakukan login. Salah satu solusi untuk mengatasinya Anda bisa mereset password tersebut.



Gambar 4.1 Klik *Create a password reset disk*

Perlu diingat *password reset disk* ini hanya bisa digunakan untuk account yang dibuatkan *reset disk*-nya. Apabila dalam komputer Anda terdapat beberapa account maka masing-masing account harus membuat *password reset disk*-nya sendiri-sendiri dan tidak bisa digunakan untuk account yang lainnya.

4.1 Membuat Password Reset Disk

Sebelum kita mulai membuat *password reset disk*, pertama-tama pastikan flashdisk Anda sudah terpasang. Baiklah langsung saja, berikut adalah cara untuk membuat *Password Reset Disk* tersebut:

1. Pertama-tama klik menu **Create a password reset disk** yang terdapat pada menu sebelah kiri halaman *User Accounts*.
2. Berikutnya akan tampil kotak dialog *Forgotten Password Wizard*, langsung saja klik tombol **Next**.



Gambar 4.2 Halaman Welcome

3. Dari tampilan nama flashdisk yang muncul apabila Anda memasang lebih dari satu flashdisk tentu saja Anda harus memutuskan untuk menggunakan salah satunya. Setelah itu, klik tombol **Next**.



Gambar 4.3 Memilih flashdisk

4. Sekarang masukkan password yang digunakan saat ini oleh account yang akan Anda buat *reset disk*-nya, lanjutkan dengan mengklik tombol **Next**.



Gambar 4.4 Memasukkan password

5. Tungguah prosesnya dilakukan berakhir. Setelah mencapai 100%, berarti proses pembuatan *password reset disk* sudah selesai dilakukan, klik kembali tombol **Next**.



Gambar 4.5 Proses pembuatan Password Reset Disk

6. Terakhir akan tampil informasi bahwa pembuatan *password reset disk* telah berhasil dilakukan, silahkan lepaskan flashdisk tersebut lalu klik tombol **Finish**.



Gambar 4.6 Proses selesai

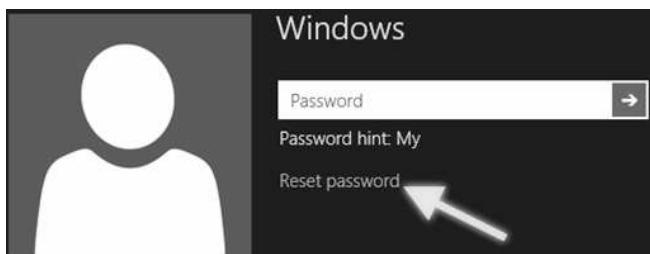
Sesudah semua langkah di atas selesai Anda lakukan maka simpanlah flashdisk tersebut di tempat yang aman. Jangan sampai jatuh ke tangan orang lain yang tidak berhak. Jika Anda membuka flashdisk tersebut maka di dalamnya akan terdapat sebuah file yang bernama *userkey.psw*.

Password reset disk ini perlu Anda buat satu kali saja. Untuk selanjutnya apabila Anda sering bergonta-ganti password asalkan masih untuk *account* yang sama maka Anda cukup menggunakan satu buah *password reset disk* ini saja. Sehingga Anda tidak perlu membuat *password reset disk* ini setiap kali ganti password.

4.2 Menggunakan Password Reset Disk

Entah apa yang terjadi, tiba-tiba Anda lupa dengan password *account* Anda. Untungnya Anda telah membuat *password reset disk*. Berikut adalah langkah untuk menggunakan *password reset disk*, apabila Anda lupa password:

1. Masukkanlah flashdisk yang merupakan *password reset disk* yang telah Anda buat sebelumnya.
2. Pada halaman *logon screen* sewaktu Anda salah memasukkan password maka akan muncul tulisan **Reset password**. Klik pada tulisan tersebut.



Gambar 4.7 Pilihan Reset password

3. Selanjutnya akan tampil kotak dialog *Password Reset Wizard*, langsung saja klik tombol **Next**.



Gambar 4.8 Halaman Welcome

4. Berikutnya Anda diminta untuk menentukan nama flashdisk yang digunakan. Terutama jika Anda memasang lebih dari satu flashdisk, lanjutkan dengan mengklik tombol **Next**.



Gambar 4.9 Memasukkan flashdisk

5. Masukkan password baru yang Anda inginkan, lalu klik **Next**.



Gambar 4.10 Memasukkan password

6. Terakhir akan tampil pesan bahwa proses reset password telah berhasil dilakukan. Klik saja tombol **Finish**.

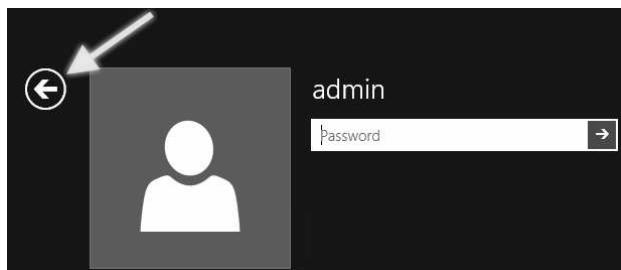


Gambar 4.11 Proses reset selesai

Kini Anda bisa login kembali menggunakan password yang baru saja Anda buat. Dan simpanlah kembali flashdisk Anda di lokasi yang aman.

4.3 Tips

Sebagai tips tambahan, apabila sewaktu Anda salah mengetikkan password namun tulisan *Reset password* tidak muncul maka cobalah Anda menampilkan nama-nama user account lainnya dengan mengklik tanda panah yang terdapat pada sudut kiri atas gambar account user.



Gambar 4.12 Mencari account yang lain

Setelah beberapa account muncul, klik kembali pada nama account Anda untuk login. Biasanya, tulisan *Reset password* akan tampil. Teapi, jika Anda masih tidak bisa menampilkan nama-nama account pada *logon screen* tersebut, restartlah komputer Anda terlebih dahulu. Lalu coba lagi login, barulah tulisan *Reset password* kembali muncul.

5 FAMILY SAFETY & EVENT VIEWER

Walaupun fitur keamanan *Family Safety* ini masih berhubungan dengan *User Accounts*, namun saya membahasnya dalam satu bab tersendiri. Supaya penjelasannya bisa menjadi lebih detil. *Family Safety* digunakan untuk merekam segala aktivitas yang dilakukan pada komputer, terutama sekali ditujukan bagi anak-anak. Misalnya, kita bisa mengetahui apa yang dilakukan sebuah account sewaktu browsing, mengatur batasan pemakaian komputer, pelarangan menjalankan program tertentu dan lain sebagainya.

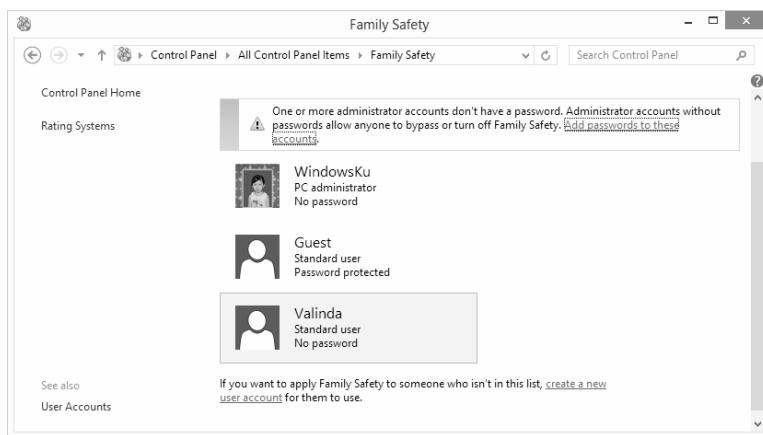
Fitur *Family Safety* ini hanya bisa diterapkan pada account standard sehingga tidak bisa diterapkan pada account yang berperan sebagai administrator. Oleh karena itu, apabila ada account administrator yang akan Anda monitor maka wajib hukumnya bagi Anda untuk mengubah statusnya menjadi standard. Pembahasan mengenai cara mengubah status account ini, sudah kita bahas dalam bab sebelumnya.

Untuk menerapkan fitur *Family Safety* ini, Anda tinggal mengklik ikon **Family Safety** yang terdapat dalam halaman Control Panel.



Gambar 5.1 Memilih Family Safety

Setelah itu, klik pada nama account yang ingin Anda terapkan *Family Safety*. Sebagai contoh di bawah ini, saya memilih account yang bernama Valinda.



Gambar 5.2 Halaman utama Family Safety

Dari tampilan berikut, berikan pilihan pada bagian **On, enforce current settings**.



Gambar 5.3 Mengaktifkan Family Safety

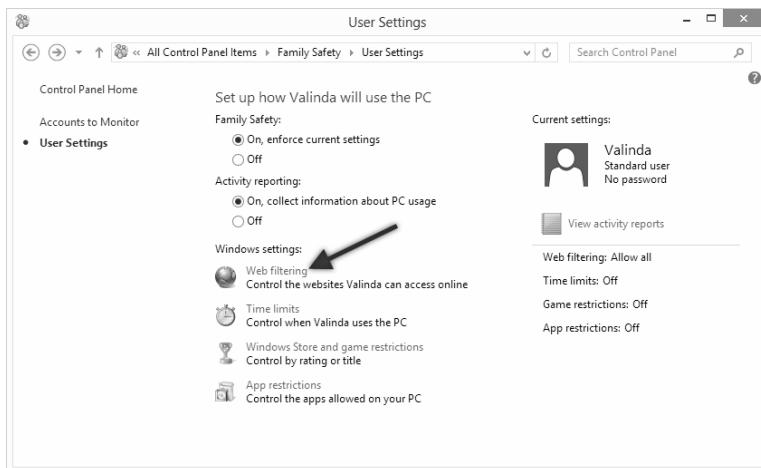
Jika diinginkan maka Anda juga bisa menerapkan pengamanan tambahan pada bagian *Windows settings*:

- *Web filtering*, berfungsi untuk mengatur website apa saja yang boleh dibuka dan tidak.
- *Time limits*, mengatur batasan waktu pemakaian komputer.
- *Windows Store and game restrictions*, pelarangan main game dan menjalankan Windows Store.
- *App restrictions*, mengatur program apa saja yang tidak boleh dijalankan.

5.1 Membatasi Akses Website

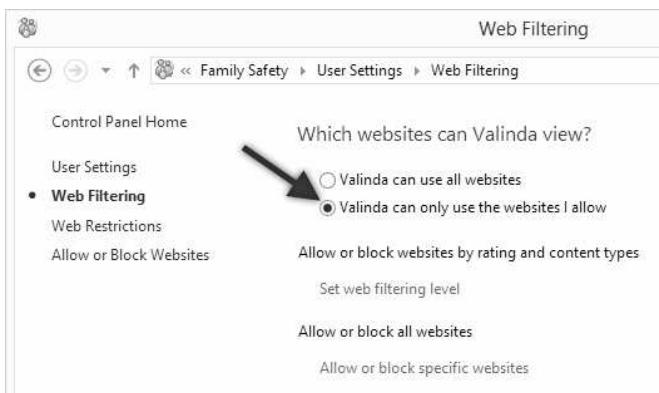
Seperti telah dijelaskan sebelumnya, *Web Filtering* berarti kita akan mengatur website apa saja yang boleh dibuka oleh sebuah account.

Langsung saja, pada halaman *User Settings*, klik pada link **Web filtering**.



Gambar 5.4 Memilih Web Filtering

Selanjutnya, pilihlah opsi Valinda can only use the websites I allow.



Gambar 5.5 Menentukan website yang diizinkan

Maka pilihan pengaturan lainnya akan menjadi aktif, dan pada panel sebelah kiri juga bertambah dua opsi lagi. Perlu Anda ketahui bahwa opsi pada panel sebelah kiri dengan link yang ada di halaman utama adalah sama saja, yaitu:

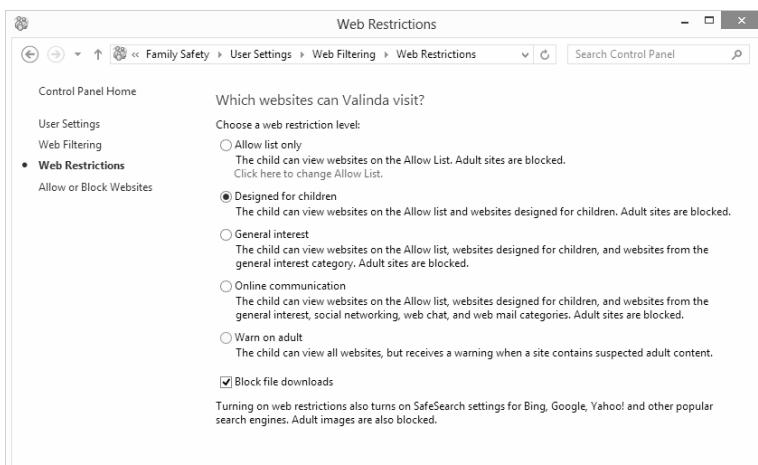
- *Web Restrictions* atau *Set web filtering level*, merupakan fungsi untuk mengizinkan atau tidak mengizinkan pengaksesan sebuah website berdasarkan isi dan rating dari website tersebut.
- *Allow or Block Websites* memiliki fungsi yang sama dengan *Allow or block spesific websites*, yaitu mengizinkan atau memblokir website tertentu.

Sebagai contoh pertama kita akan mencoba menerapkan akses sebuah website berdasarkan isi atau rating dari sebuah website, Anda bisa mengklik *Web Restrictions* atau *Set web filtering level*. Secara default, fasilitas ini akan memblokir semua website untuk orang dewasa, dan juga mengaktifkan semua mesin pencari, hanya saja dengan menghilangkan semua *image* yang mengandung gambar orang dewasa (maksudnya gambar porno).

Dari tampilan berikutnya maka terdapat beberapa opsi yang bisa Anda pilih salah satunya untuk diterapkan. Berikan pilihan Anda pada salah satu opsi yang tersedia:

- *Allow list only*, berarti user hanya bisa mengakses website yang telah dibuat daftarnya terlebih dahulu. Semua website dewasa/porno akan diblokir.

- *Designed for children*, user hanya menampilkan website yang terdapat pada daftar *Allow list* ditambah dengan website yang dirancang khusus untuk anak-anak. Untuk website dewasa/porno akan diblokir.
- *General interest*, user dapat menampilkan website yang terdapat pada daftar *Allow list*, ditambah dengan website yang di-desain untuk anak-anak, serta website yang dikategorikan untuk umum. Sedangkan website dewasa/porno akan diblokir.
- *Online communication*, user dapat menampilkan website yang terdapat pada daftar *Allow list* ditambah dengan website yang dirancang untuk anak-anak, website yang dikategorikan untuk umum, jejaring sosial, serta website yang tergolong web chat dan web mail. Untuk website dewasa/porno akan tetap diblokir.
- *Warn on adult*, user dapat menampilkan semua website, hanya saja akan menerima pesan peringatan apabila diduga website tersebut mengandung konten dewasa.



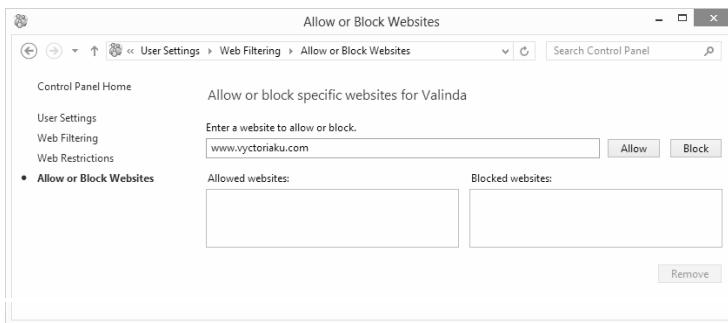
Gambar 5.6 Menentukan pembatasan

Jika Anda tidak memberikan tanda centang pada bagian **Block file downloads** maka user bisa melakukan download sewaktu menggunakan internet. Tapi jika Anda tidak mengizinkan seorang user untuk melakukan download maka centanglah pada bagian **Block file downloads**.

Apabila Anda ingin mengaktifkan opsi *Allow list only* maka Anda harus membuat daftar (*list*) website-nya terlebih dahulu. Caranya adalah dengan mengklik link **Click here to Change Allow List**.

Dari halaman berikutnya yang tampil ketiklah nama sebuah website. Lalu pada bagian sebelah kanan klik pada salah satu tombol:

- *Allow* berarti website tersebut bisa diakses.
- *Block* berarti website tersebut tidak boleh diakses (diblokir).



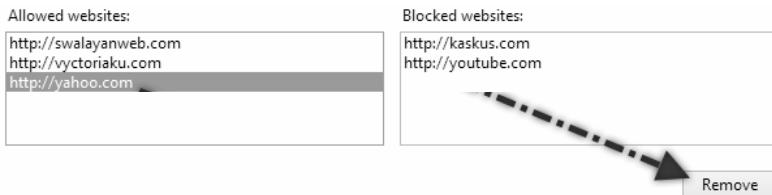
Gambar 5.7 Menentukan website yang bisa diakses

Apabila Anda mengklik tombol *Allow* maupun tombol *Block* maka nama website tersebut akan masuk pada kolom yang telah disediakan. Lakukan lagi untuk nama website lainnya.



Gambar 5.8 Daftar website yang diizinkan dan diblokir

Jika Anda secara tidak sengaja salah ketik, atau salah menempatkan sebuah website maka Anda bisa menghapus atau mengeluarkannya dari salah satu kolom tersebut. Anda tinggal mengklik pada nama yang akan dihapus, lalu klik tombol **Remove**.



Gambar 5.9 Menghapus website dari daftar

Setelah Anda mengatur nama-nama website yang boleh dibuka maupun tidak, barulah kemudian Anda bisa memilih opsi *Allow list only*. Harap diingat, apabila Anda sudah mengatur *Allow list* di atas maka opsi lainnya yang tersedia tetap akan mengikuti aturan berdasarkan nama website yang telah Anda buat tersebut.

5.2 Mengatur Waktu Pemakaian Komputer

Sekarang kita akan mengatur waktu akses pemakaian sebuah komputer untuk sebuah account, atau kapan saja sebuah account bisa mengakses sebuah komputer. Pertama-tama Anda harus memilih pilihan **Time limits**.

Dari panel sebelah kiri terdapat dua pilihan yang disediakan, yaitu:

- *Time Allowance*, yang digunakan untuk mengatur berapa lama waktu pemakaian komputer yang diizinkan per hari.
- *Curfew*, digunakan untuk mengatur waktu pemakaian berdasarkan waktu atau jam tertentu.

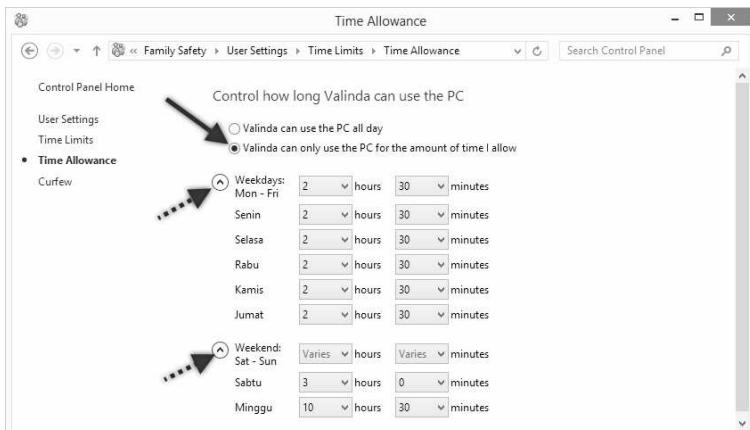
Control Panel Home	Control when Valinda can use the PC
User Settings	Set the number of hours Valinda can use the PC per day
• Time Limits	
Time Allowance	Set time allowance
Curfew	Set the time of day Valinda can use the PC
	Set curfew

Gambar 5.10 Time Limits

Sebagai contoh pertama kita akan mengatur waktu pemakaian berdasarkan berapa lama sebuah account boleh menggunakan komputer. Untuk melakukan hal ini, klik pada **Time Allowance** atau **Set time allowance**.

Dari pilihan berikutnya yang diberikan, pilihlah **Valinda can only use the PC for the amount of time I allow**. Maka di bawahnya akan tampil pilihan hari kerja dan akhir pekan. Apabila Anda ingin menampilkan keseluruhan harinya maka klik pada tanda panah kecil yang berada dalam lingkaran.

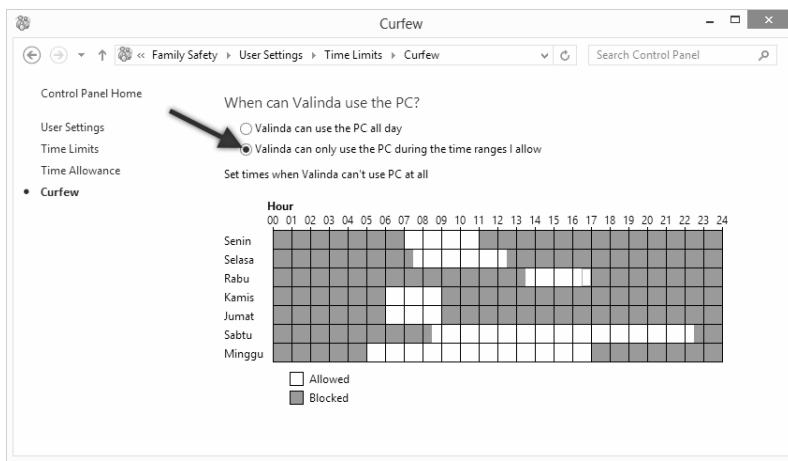
Pada gambar di bawah ini saya mengatur pemakaian komputer hanya bisa dilakukan selama 2,5 jam untuk hari Senin sampai Jum'at, untuk hari Sabtu selama 3 jam, dan hari Minggu selama 10,5 jam.



Gambar 5.11 Menentukan durasi pemakaian komputer

Sekarang kita akan mengatur pemakaian komputer berdasarkan jam pemakaian, dari jam berapa sampai jam berapa. Untuk melakukan hal ini, klik pada menu **Curfew**.

Dalam tampilan berikutnya, berikan pilihan pada bagian **Valinda can only use the PC during the time ranges I allow**. Maka di bawahnya akan tampil nama hari beserta tabel jam pemakaian komputer. Yang harus Anda lakukan adalah memblok kotak-kotak jam yang tersedia. Untuk warna biru berarti pada jam tersebut tidak diizinkan, sebaliknya warna putih adalah jam-jam yang diperbolehkan untuk mengakses komputer.



Gambar 5.12 Menentukan jam pemakaian

Sebagai penjelasan dari gambar di atas saya telah mengatur pada hari Senin, komputer hanya bisa digunakan dari jam 7:00 sampai dengan jam 11:00. Sedangkan untuk hari Selasa komputer bisa digunakan dari jam 7:30 sampai dengan jam 12:30. Untuk hari lainnya, silahkan Anda lihat sendiri.

5.3 Batasan Pemakaian Windows Store dan Game

Sekarang kita akan membahas batasan pemakaian Windows Store dan Game pada Windows 8. Anda bisa membatasinya berdasarkan rating atau judul. Langsung saja, untuk menggunakan fitur keamanan yang satu ini, klik pada pilihan **Windows Store and game restrictions**. Yang diikuti dengan memberikan pilihan pada bagian **Valinda can only use games and Windows Store app I allow**. Maka di bawahnya akan diaktifkan dua pilihan pengaturan.



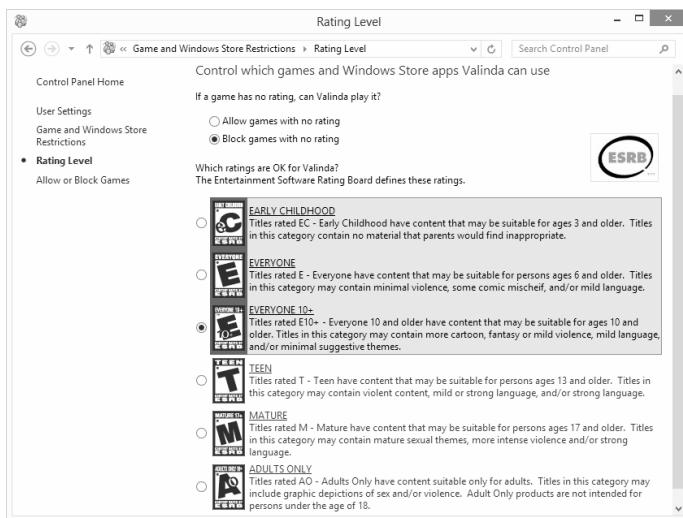
Gambar 5.13 Pembatasan game dan aplikasi

Pertama-tama kita akan membatasi pemakaian berdasarkan rating. Klik saja pada **Rating Level** yang terdapat pada panel sebelah kiri atau pada bagian *Set game and Windows Store ratings* yang berada di tampilan utama.

Dari pilihan berikutnya yang tampil, Anda bisa menentukan apakah akan memblokir game yang tidak memiliki rating dengan memilih **Block games with no rating**.

Atau Anda juga bisa membiarkan Windows untuk mengizinkan semua game tanpa rating dengan memilih *Allow game with no rating*, tentu saja pilihan ini tidak begitu bagus karena semua game termasuk game dewasa bisa dimainkan nantinya.

Selain itu, di bawahnya juga terdapat pilihan rating game, pilihlah rating yang Anda inginkan. Sebagai contoh di bawah ini, saya memberikan pilihan pada bagian *EVERYONE 10+*, arti game dengan rating tersebut cocok untuk orang dengan usia 10 tahun atau lebih. Game seperti ini seperti kartun, fantasi dan sebagainya. Hal ini juga secara otomatis kita bisa menggunakan atau memainkan yang ratingnya di bawahnya, yaitu *EARLY CHILDHOOD* dan *EVERYONE*.



Gambar 5.14 Rating game

Jika dilihat dari segi umur maka rating game tersebut digunakan untuk usia yang berbeda-beda:

- *Early Childhood* untuk anak-anak berusia 3 tahun
- *Everyone* untuk anak berusia 6 tahun
- *Everyone 10+* untuk anak berusia 10 tahun
- *Teen* untuk remaja, rentang usia sekitar 13 tahun
- *Mature* untuk yang telah berusia 17 tahun
- *Adults Only* untuk yang telah berusia lebih dari 18 tahun

Rating tersebut diambil berdasarkan pemeringkatan oleh *The Entertainment Software Rating Board (ESRB)*.



Gambar 5.15 Logo ESRB

Kedua pilihan di atas bisa Anda gabungkan atau berdiri sendiri-sendiri, antara pemakaian rating dan juga memblokir atau mengizinkan game yang tidak menggunakan rating.

Pengaturan berikutnya yang bisa Anda terapkan adalah dengan langsung menentukan game apa saja yang boleh dan game apa saja yang tidak boleh dimainkan. Untuk melakukan hal ini, klik pada **Allow or block games** yang terdapat pada panel sebelah kiri.

Langkah berikutnya, berikan pilihan pada bagian *Always allow* untuk game yang boleh dimainkan, atau sebaliknya *Always block* untuk game yang tidak boleh dimainkan. Sedangkan untuk kolom *User rating setting*, akan tergantung pada setting rating yang telah Anda atur sebelumnya. Jika game tersebut tergolong pada rating yang Anda pilih maka game tersebut bisa dimainkan. Jika game tersebut rating-nya tidak memenuhi apa yang Anda tentukan maka game tersebut tidak dapat dimainkan.

Title/Rating	Status	User rating setting	Always allow	Always block
3D Pinball - Space Cadet No rating provided	Can play	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Angry Birds No rating provided	Can play	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Angry Birds Star Wars No rating provided	Can play	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Chess Titans E	Can play	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
FreeCell E	Can't play	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Hearts E	Can't play	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Hold 'Em T: Simulated gambling	Can't play	<input type="radio"/>	<input type="radio"/>	<input checked="" type="checkbox"/>
InkBall E	Can't play	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Internet Backgammon E: Online rating notice	Can't play	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Internet Checkers E: Online rating notice	Can't play	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Internet Spades E: Online rating notice	Can't play	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Mahjong Titans E	Can't play	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Microsoft® Tinker™ E	Can't play	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Minesweeper E	Can't play	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
More Games from Microsoft No rating provided	Can't play	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
More Games from Steam	Can't play	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>

Gambar 5.16 Spesifik game

Untuk tambahan informasi, ada banyak standar yang membuat rating sebuah game, selain rating menurut ESRB yang telah kita gunakan di atas. Standar rating lainnya yang bisa Anda terapkan untuk digunakan;

bukalah halaman pertama *Family Settings*. Lalu klik link **Rating Systems** yang berada pada panel sebelah kiri.



Gambar 5.17 Rating Systems

Kemudian pilihlah salah satu standar rating yang ingin Anda gunakan.

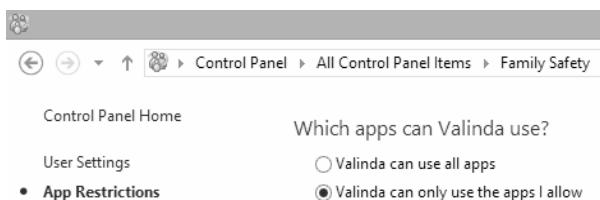


Gambar 5.18 Jenis-jenis sistem rating

5.4 Memblokir Aplikasi

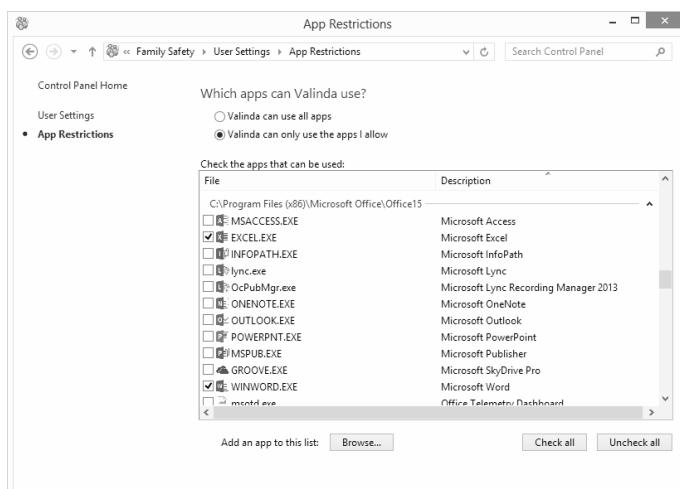
Kali ini kita akan mengatur program apa saja yang boleh digunakan dan apa saja yang tidak. Sebagai contoh di sini kita akan mengatur supaya user dengan account standar hanya boleh membuka Microsoft Word dan Microsoft Excel saja, maka klik pada **App restrictions**.

Dan dari halaman berikutnya yang tampil, berikan pilihan pada **Valinda can only use the apps I allow**.



Gambar 5.19 Menentukan program yang diizinkan

Tungguhlah proses menampilkan semua program dalam komputer Anda. Diikuti dengan memberikan tanda centang pada program yang boleh digunakan.

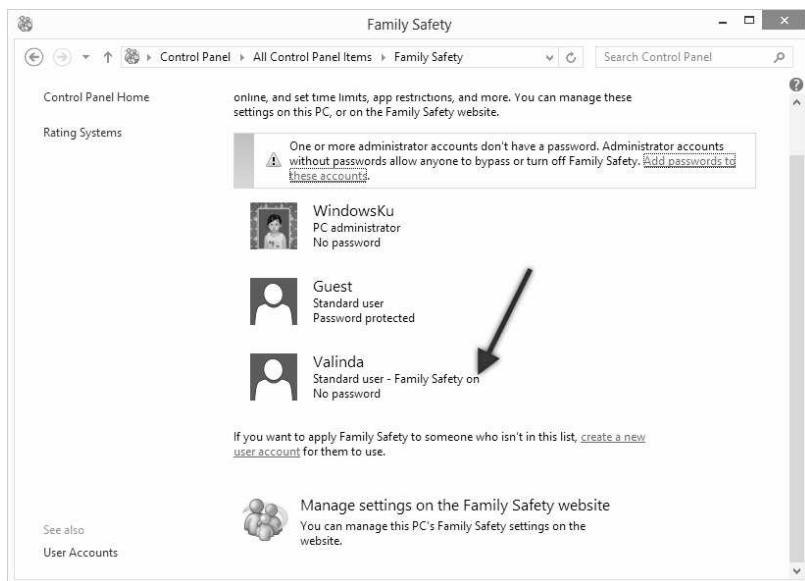


Gambar 5.20 Daftar program

Setelah pengaturan *Family Safety* selesai Anda lakukan, Anda cukup menutup jendela kerja tersebut maka semua setting akan disimpan, tanpa harus menekan tombol *Save* atau tombol apapun.

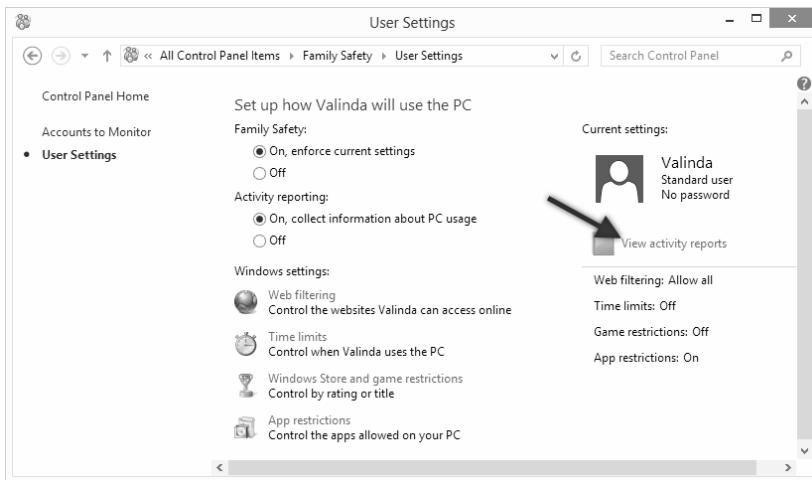
5.5 Melihat Aktivitas Pemakaian

Setelah selesai mengatur *Family Safety*, tutup saja halaman tersebut. Sewaktu Anda menampilkan halaman pertama *Family Safety*, terdapat pesan *Family Safety on*. Hal ini berarti account tersebut bisa dimonitor oleh account administrator.



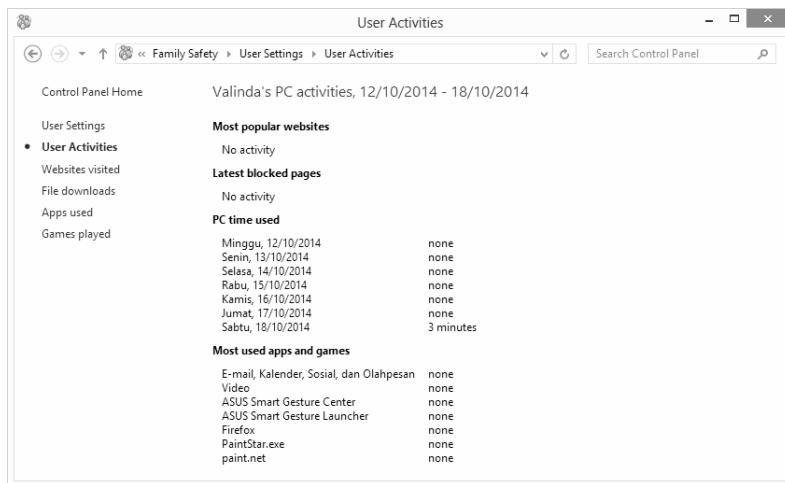
Gambar 5.21 *Family Safety aktif*

Selanjutnya, untuk mengetahui aktivitas yang dilakukan oleh sebuah account. Pada halaman utama *Family Safety*, klik pada account yang terdapat tanda *Family Safety on*. Selanjutnya, perhatikan pada bagian sebelah kanan dan klik pada **View activity reports**.



Gambar 5.22 View activity reports

Dari halaman berikutnya yang tampil, Anda bisa melihat kapan saja user tersebut mengakses sebuah komputer dan juga durasi pemakaiannya. Dan pada bagian *Most used apps and games*, menunjukkan program yang sering digunakan.



Gambar 5.23 Daftar pemakaian komputer

Sekarang perhatikan pada panel sebelah kiri dan klik pada **App used**. Dari hasil yang ditampilkan maka Anda bisa melihat program apa saja yang diblokir, beserta waktu pengaksesannya.

Apps used				
	Name	Times used	Action taken	Last used
Control Panel Home	Video	1	Blocked	18/10/2014 8:36 none
User Settings	Firefox	2	Blocked	18/10/2014 8:36 none
User Activities	paint.net	1	Blocked	18/10/2014 8:36 none
Websites visited	PaintStar.exe	1	Blocked	18/10/2014 8:35 none
File downloads	E-mail, Kalender, Sosial, dan Olahpesan	1	Blocked	18/10/2014 8:34 none
● Apps used	ASUS Smart Gesture Center	27	Blocked	18/10/2014 8:34 none
Games played	ASUS Smart Gesture Launcher	1	Blocked	18/10/2014 8:34 none

Gambar 5.24 Daftar program yang digunakan

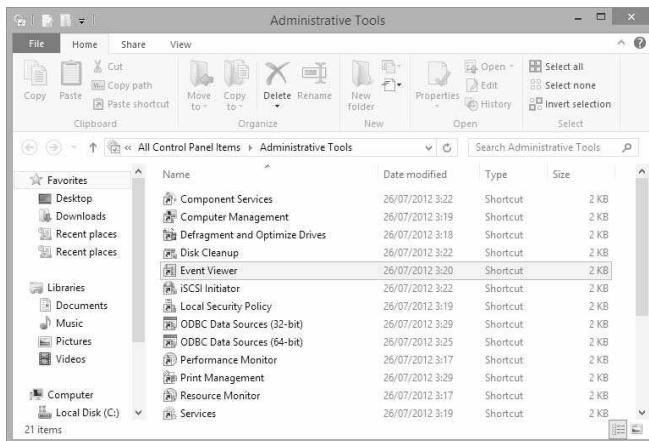
Berikutnya, Anda bisa melihat sendiri berbagai laporan lainnya dari menu yang telah disediakan.

5.6 Event Viewer

Jika fitur *Family Safety* digunakan untuk mengamankan account orang lain supaya tidak mengakses website terlarang atau membuka program tertentu. Kemudian kita bisa melihat aktivitas apa yang dilakukan oleh sebuah account. Sebagai tambahan untuk bab ini, kita juga perlu melihat *event* atau kegiatan apa saja yang telah dilakukan dalam komputer.

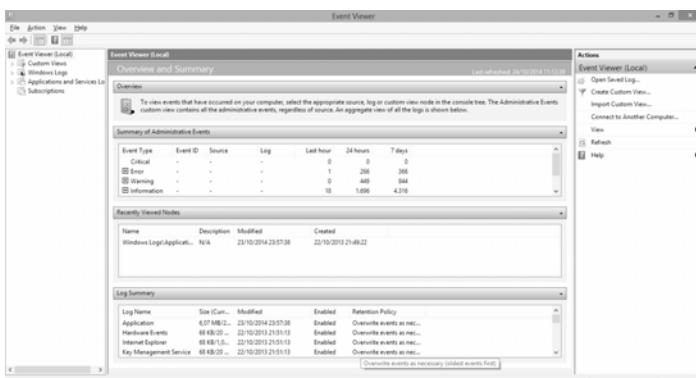
Sebuah tool bernama Event Viewer bertugas untuk mencatat kegiatan (*event*) apa saja yang terjadi dalam komputer. Dengan adanya fasilitas ini maka kita bisa memantau kegiatan dalam komputer kita, terutama untuk masalah keamanan data, dan juga *troubleshooting* terhadap suatu masalah. Dalam bagian ini, saya akan menjelaskan mengenai Event Viewer secara global saja.

Untuk menjalankan Event Viewer, bukalah Control Panel lalu klik **Administrative Tools**. Dalam jendela kerja *Administrative Tools* terdapat banyak pilihan yang tersedia. Di sini kita cukup klik **Event Viewer**.



Gambar 5.25 Administrative Tools

Sewaktu Anda membuka Event Viewer maka akan tampil halaman *Overview and Summary* yang berisikan garis besar kegiatan apa saja yang dilakukan dalam komputer Anda.



Gambar 5.26 Event Viewer

Event dibagi menjadi lima jenis, yaitu:

- *Critical* (gawat)
- *Error* (terjadi kesalahan normal/biasa)
- *Warning* (peringatan)

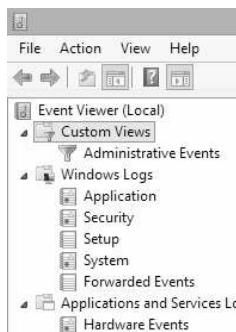
- *Information* (informasi umum)
- *Audit Success* (pemeriksaan berhasil dilakukan)
- *Audit Failure* (pemeriksaan gagal)

Event Type	Event ID	Source	Log	Last hour	24 hours	7 days
Critical	-	-	-	0	0	0
Error	-	-	-	1	266	366
Warning	-	-	-	0	449	844
Information	-	-	-	18	1.696	4.316

Gambar 5.27 Jenis event

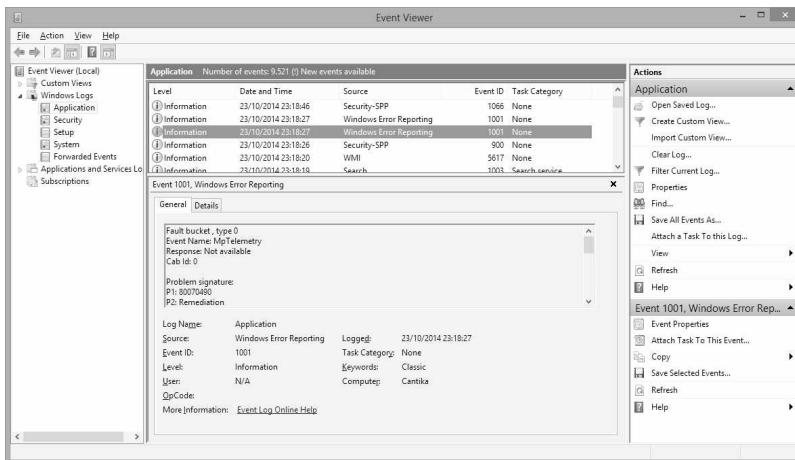
Pada panel sebelah kiri, terdapat beberapa hal berikut:

- *Custom Views*, bagian ini menangani perintah yang pernah dilakukan oleh user.
- *Windows Log*, berisikan pencatatan mengenai kegiatan yang dilakukan oleh Windows
- *Application and Services Logs*, bagian ini berisikan pencatatan tentang pemakaian aplikasi dan servis.
- *Subscriptions*, untuk mengaktifkan pilihan ini maka Anda harus menjalankan servis yang bernama *Windows Event Collector Service*.



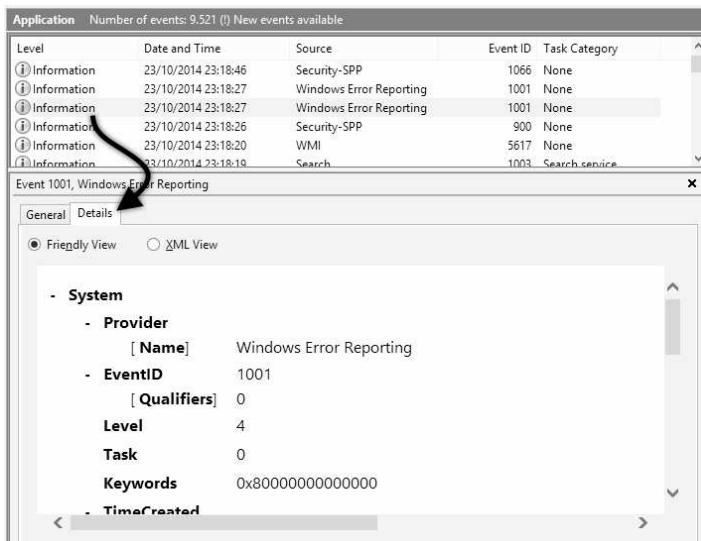
Gambar 5.28 Menu Event Viewer

Sebagai contoh, kita akan melihat isi log dari *Windows Logs*, tepatnya pada bagian *Application*. Misalnya, kita klik *Information* yang tanggal 23/10/2014 jam 23:18:27 mengenai *Windows Error Reporting*. Maka di bawahnya akan tampil informasi mengenai bagian tersebut.



Gambar 5.29 Informasi Event

Apabila Anda ingin mengetahui informasi lebih detail klik tombol **Details**.



Gambar 5.30 Informasi detail

Itulah cara menggunakan Event Viewer yang fungsinya hanya untuk menampilkan (*viewer*) aktivitas (*event*) yang dilakukan dalam komputer.

5.7 Tips

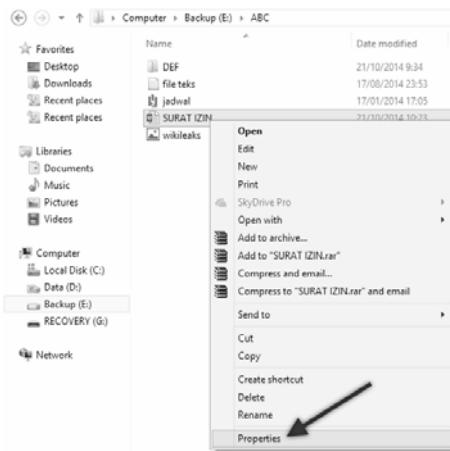
Untuk mencegah anggota keluarga Anda yang ikut menggunakan komputer secara bersama. Selain memasang account standard, sebaiknya, Anda juga mengaktifkan fitur *Family Safety*, supaya Anda bisa memantau tindakan yang dilakukan oleh anggota keluarga. Terutama dalam menghindari akses internet yang mengandung konten dewasa maupun website negatif lainnya.

6 KEAMANAN FILE DAN FOLDER

Windows 8 menggunakan NTFS untuk mengatur sistem file-nya. Sehingga sistem keamanannya pun lebih baik dari pada sistem FAT atau FAT32. Dengan menerapkan NTFS maka salah satu fitur keamanan tambahan yang terdapat pada Windows 8 adalah pengamanan file dan folder. Hal ini bisa dilihat dari kotak dialog *Properties* yang terdapat sebuah tab dengan nama *Security* yang berfungsi untuk mengamankan folder maupun file.

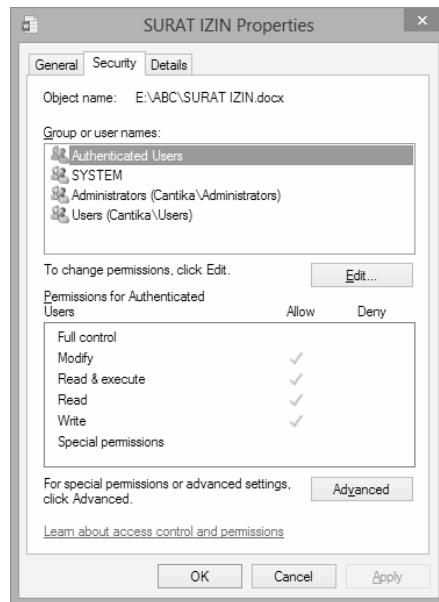
Metode pengamanan file dan folder seperti yang dijelaskan disebut dengan nama *Access Control List* (ACL). ACL adalah sebuah metode pengaturan user dalam menangani sebuah objek. Objek di sini bisa berupa file, folder, program dan sebagainya yang terdapat dalam Windows. Penanganan objek bisa diantaranya, pengaturan apakah sebuah objek tidak boleh dibuka, hanya boleh dibaca (*read*), bisa ditulis (*write*), dan apakah bisa dieksekusi (*execute*).

Untuk menampilkan kotak dialog *Properties*, dalam File Explorer (untuk versi Windows sebelum Windows 8, namanya Windows Explorer). Klik kanan pada sebuah folder maupun file kemudian dari menu yang muncul, klik **Properties**.



Gambar 6.1 Menu klik kanan

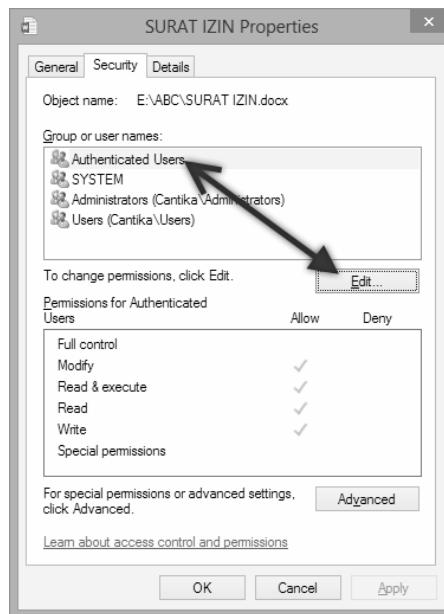
Diikuti dengan munculnya kotak dialog *Properties* lalu klik tab **Security** untuk mengatur pengamanan tambahannya.



Gambar 6.2 Kotak dialog properties

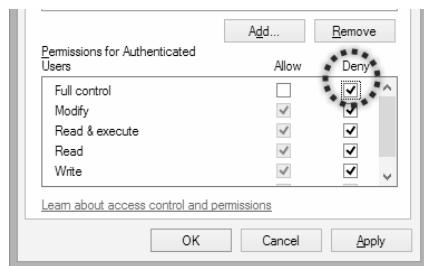
6.1 Melarang Akses File & Folder

Baiklah, mari kita mulai dan lihat apa saja yang bisa kita lakukan pada bagian ini. Tampilkan kotak dialog *Properties* untuk sebuah file. Kemudian buka tab *Security*. Pastikan user yang terpilih adalah *Authenticated Users*, lalu klik tombol **Edit**.



Gambar 6.3 Tab *Security*

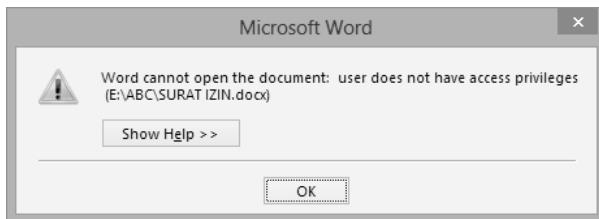
Dalam kotak dialog berikutnya yang bernama *Permissions for <nama file>*, berikan tanda centang pada kolom **Deny** tepatnya pada baris *Full Control*. Secara otomatis, semua pilihan di bawahnya akan ikut tercentang. Setelah selesai, klik tombol **Apply**.



Gambar 6.4 Memilih Deny

Berikutnya akan tampil kotak dialog konfirmasi perubahan, klik saja **Yes**. Setelah Anda kembali pada kotak dialog sebelumnya, klik **OK** sampai semua kotak dialog tertutup.

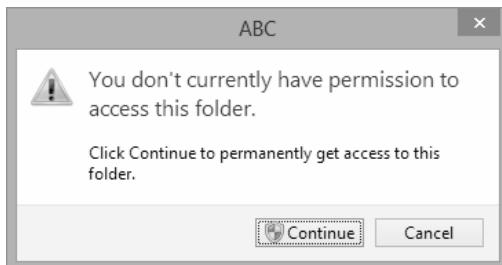
Terakhir, cobalah membuka file tersebut. Kini file-nya tidak bisa dibuka. Yang muncul adalah kotak dialog dengan pesan user tidak memiliki hak akses.



Gambar 6.5 Tidak bisa membuka file dokumen

Tidak hanya itu, file tersebut juga tidak akan bisa disalin lagi baik ke dalam flashdisk maupun ke dalam drive lainnya. Alhasil data kita akan menjadi aman.

Dengan cara yang sama pula kita bisa menerapkan tindakan di atas pada sebuah folder. Sehingga folder tersebut tidak bisa dibuka, tentu saja data kita yang berada dalam folder tersebut menjadi aman.



Gambar 6.6 Folder tidak bisa dibuka

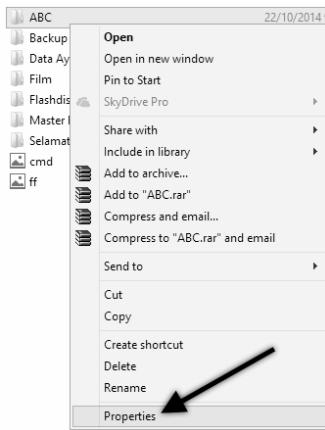
6.2 Enkripsi File & Folder

Masih berhubungan dengan file dan folder yang terdapat dalam komputer kita. Sekarang kita akan mengenkripsi file maupun folder, yang tentu saja fungsinya untuk lebih mengamankan lagi file atau folder tersebut. Langkah awal melakukan enkripsi ini tidak jauh beda seperti mengatur *Permissions* di atas.

Apa yang akan kita lakukan dalam bagian ini disebut sebagai *Encrypting File System (EFS)*. Prinsip kerja dari EFS tidak jauh berbeda dengan kebanyakan metode enkripsi yang pernah ada. Di mana sewaktu pertama kali melakukan enkripsi, Windows akan membuat sebuah sertifikat (*certificate*) yang disertai dengan file kunci enkripsi (*key*). Kedua hal tersebut digunakan oleh EFS untuk melakukan proses enkripsi dan dekripsi (membuka enkripsi). Prosesnya adalah setiap kali file ditutup maka ia akan di-enkripsi dan sewaktu dibuka file tersebut di-dekripsi.

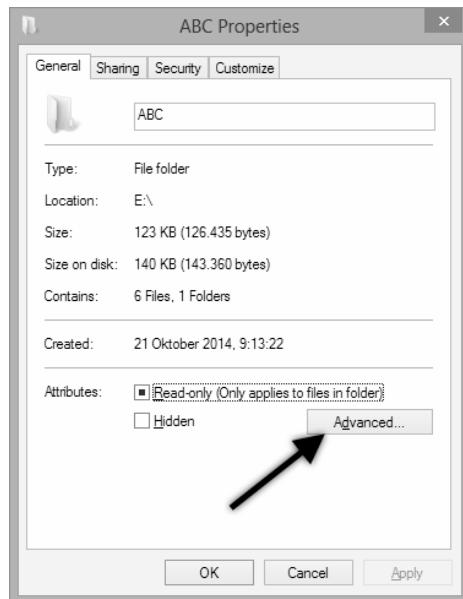
Tanpa banyak basa-basi, baiklah langsung saja, berikut langkah untuk mengenkripsi sebuah file atau folder.

1. Dalam Windows Explorer, klik kanan pada folder yang akan di-enkripsi. Sebagai contoh di sini saya akan mengenkripsi folder "ABC", selanjutnya dari menu yang muncul, klik **Properties**.



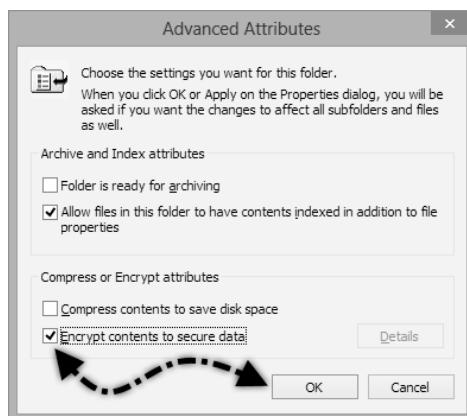
Gambar 6.7 Memilih Properties

2. Dalam kotak dialog *Properties* yang muncul, klik pada tombol **Advanced**.



Gambar 6.8 Klik Advanced

3. Proses berikutnya adalah memberikan tanda centang pada bagian **Encrypt contents to secure data** pada kotak dialog *Advanced Attributes*, diikuti dengan mengklik tombol **OK**.



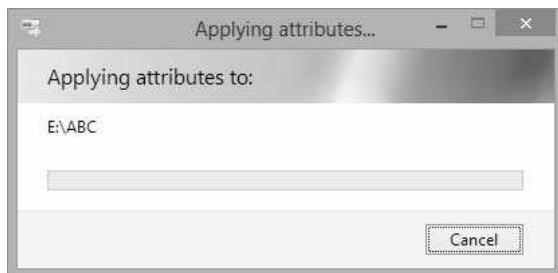
Gambar 6.9 Memilih enkripsi

4. Sekembalinya Anda pada kotak dialog sebelumnya, klik lagi tombol **OK**. Maka akan muncul kotak dialog *Confirm Attribute Changes*. Dalam kotak dialog konfirmasi tersebut akan menanyakan “Apakah Anda ingin mengenkripsi hanya folder ini saja, atau termasuk juga file dan subfolder yang berada di dalamnya”. Demi keamanan data kita, maka pilihlah pilihan yang kedua, yaitu **Apply changes to this folder, subfolders and files**. Lanjutkan dengan mengklik **OK** lagi.



Gambar 6.10 Menerapkan enkripsi pada isi folder

5. Sekarang tunggu lah proses enkripsi dilakukan hingga selesai.



Gambar 6.11 Proses enkripsi

Setelah selesai maka Anda dibawa kembali pada halaman File Explorer atau disebut juga Windows Explorer. Jika Anda perhatikan untuk file atau folder yang telah di-enkripsi maka warna font-nya akan menjadi hijau. Bukan hitam lagi, seperti folder lainnya yang normal dengan warna hitam. Hal ini akan berefek sama dengan semua file dan subfolder yang berada di dalamnya, warna font-nya akan menjadi hijau, ini menandakan bahwa proteksi enkripsi sudah aktif.

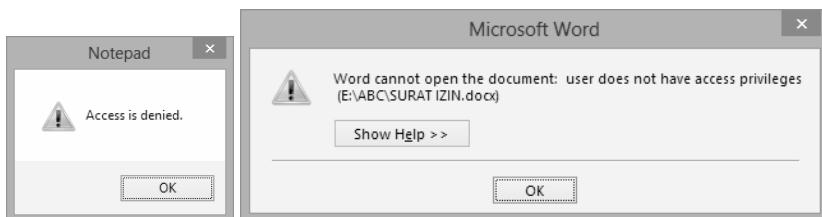


Gambar 6.12 Folder ABC sudah dienkripsi

Walaupun sudah Anda enkripsi, semua file dan subfolder di dalamnya tetap akan tampil secara normal. Kalau Anda membuka file atau folder yang sudah di-enkripsi tadi maka file tersebut akan tetap dapat terbuka dengan normal. Sebab, memang bukan itu fungsi dari enkripsi yang dilakukan. File yang telah di-enkripsi tidak akan bisa dibuka oleh account lain, baik dalam satu komputer maupun dalam sebuah jaringan.

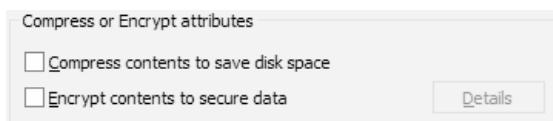
Walaupun Anda menaruh file tersebut pada drive D: atau E: yang bisa dilihat oleh umum, file tersebut tetap tidak akan bisa dibuka, kecuali oleh account Anda sendiri yang menerapkan enkripsi tersebut.

Berikut contoh pelarangan akses terhadap file teks yang akan dibuka dengan Notepad, dan juga file dokumen MS. Word.



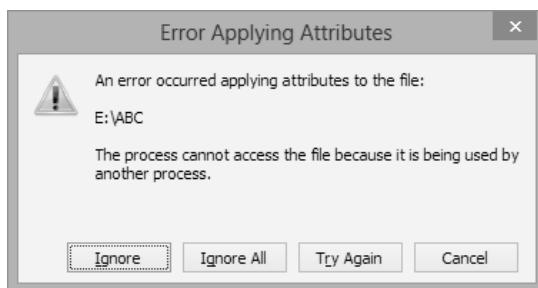
Gambar 6.13 Dilarang mengakses file teks dan dokumen

Untuk menghilangkan enkripsi tersebut dan kembali seperti sedia kala maka Anda cukup menghilangkan tanda centang pada bagian **Encrypt contents to secure data**.



Gambar 6.14 Encrypt contents to secure data

Mungkin Anda berpikiran, bisa saja account lain yang menghilangkan tanda centang tersebut sehingga bisa membuka file yang telah Anda enkripsi. Praduga Anda ternyata tidak benar, sebab account lain tetap tidak bisa melepas enkripsi yang telah dipasang. Sebab, ketika akan melepas enkripsi tersebut akan tampil error pesan seperti di bawah ini.



Gambar 6.15 Account lain dilarang mengubah enkripsi

Bahkan apabila account lain dalam komputer Anda tetap tidak bisa membuka enkripsi tersebut. Hanya account yang mengenkripsi file dan folder itu saja yang bisa membukanya.

6.3 Backup Key Enkripsi

Walaupun penerapan enkripsi adalah sesuatu yang bagus, namun hal ini akan menjadi malapetaka ketika file kunci (*key*) hilang. Apabila file kunci telah hilang, tentu saja kita tidak akan dapat membuka file yang telah kita enkripsi tersebut. Salah satu solusinya yang bisa kita lakukan adalah mem-backup key enkripsi.

Supaya lebih jelas, untuk membackup key enkripsi, ikuti langkah berikut:

1. Bukalah Control Panel dan jalankan **Internet Options**.
2. Dalam kotak dialog *Internet Options*, klik pada tab **Contents**.



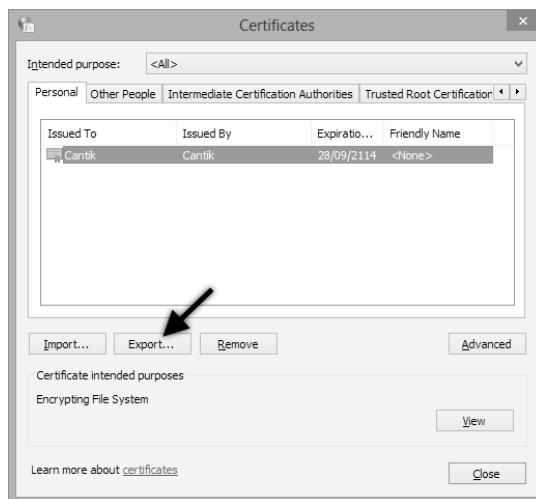
Gambar 6.16 Tab Content

3. Perhatikan pada bagian *Certificates*, klik tombol **Certificates**.



Gambar 6.17 Klik *Certificates*

4. Dari kotak dialog *Certificates*, jika dalam kotak dialog tersebut terdapat beberapa nama klik pada salah satu yang Anda gunakan. Lalu klik tombol **Export**.



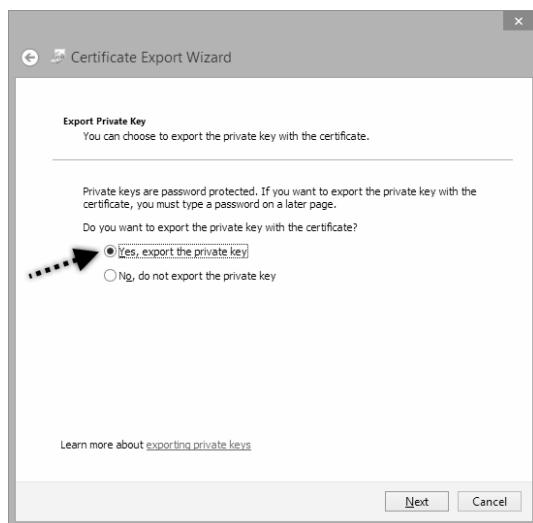
Gambar 6.18 Klik tab *Export*

5. Berikutnya akan tampil kotak dialog *Certificate Export Wizard*, langsung saja klik tombol **Next**.



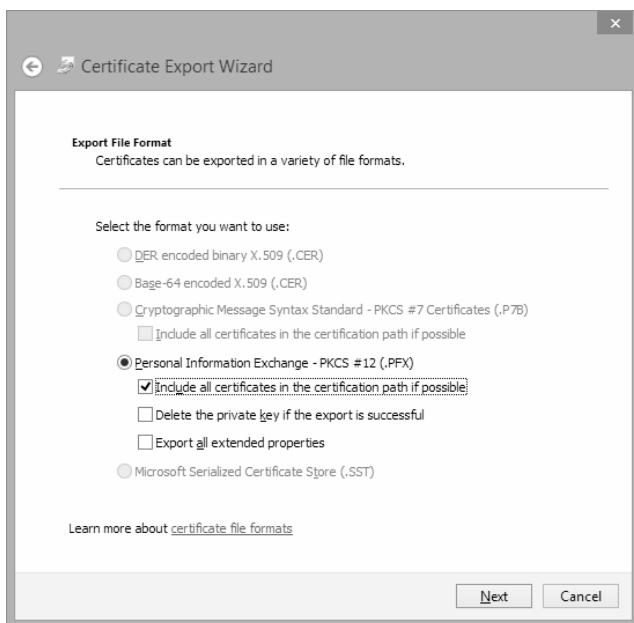
Gambar 6.19 Tampilan Welcome

6. Berikutnya pilih Yes, export the private key. Lanjutkan dengan mengklik tombol Next.



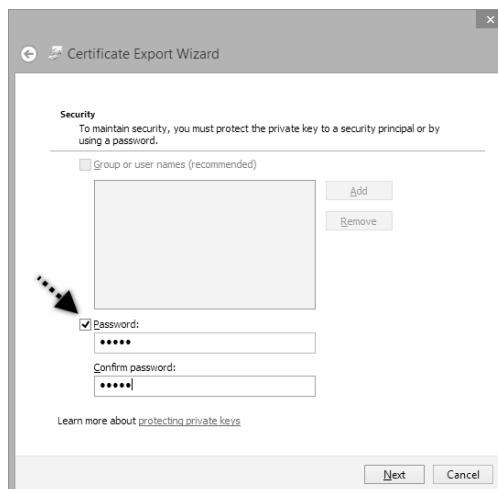
Gambar 6.20 Memilih Yes, export the private key

7. Sekarang Anda diminta untuk menentukan format file yang akan digunakan. Pilihlah **Personal Information Exchange – PKC # 12 (.PFX)**, dan klik tombol **Next**. Penjelasan mengenai format file akan saya jelaskan diakhir subbab ini.



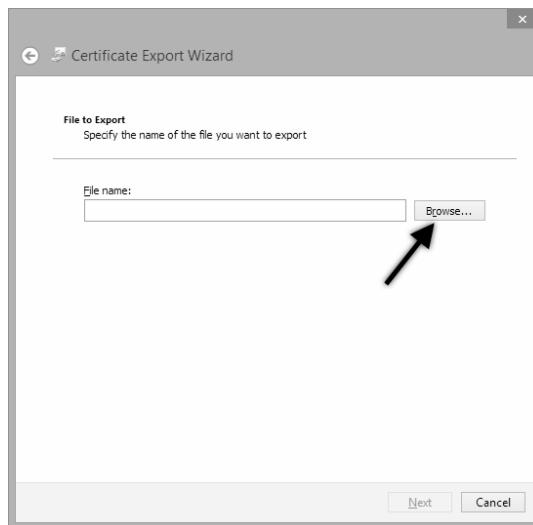
Gambar 6.21 Memilih format file

8. Untuk menjaga *key* yang Anda eksport maka file tersebut perlu diproteksi dengan password. Pertama-tama berikan tanda centang pada bagian **Password**, kemudian masukkan password yang Anda inginkan. Ulangi mengetik password yang sama pada bagian **Confirm password**. Harap diingat password yang telah Anda masukkan, sebab jika lupa maka bisa-bisa file Anda tidak bisa terbuka nantinya. Setelah selesai, klik tombol **Next**.



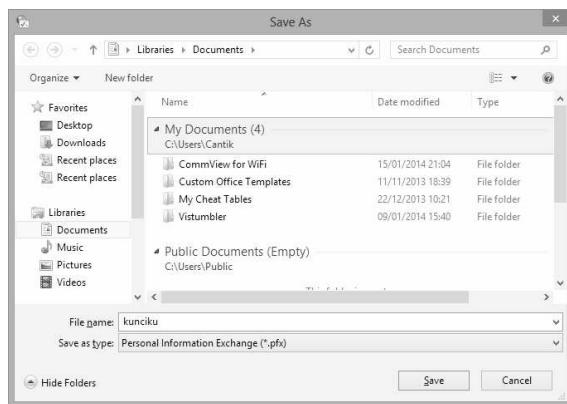
Gambar 6.22 Membuat password

9. Langkah berikutnya, Anda diminta untuk memasukkan nama file serta lokasi untuk menyimpan file tersebut. Klik pada tombol **Browse** lalu carilah di mana Anda ingin menaruh file key tersebut.



Gambar 6.23 Mencari path

10. Dalam kotak dialog *Save as* yang muncul, tentukanlah di mana folder penyimpanan file *key* tersebut. Lalu ketiklah nama file yang Anda inginkan. Sebagai contoh pada gambar di bawah ini saya menggunakan nama “kunciku” dan memilih folder “Documents”. Setelah selesai, klik tombol **Save**.



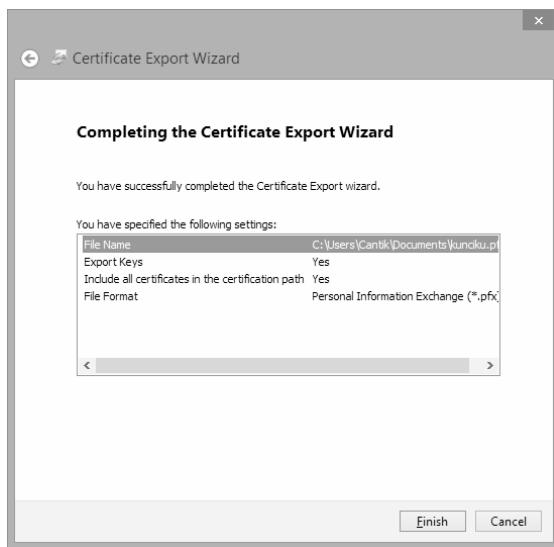
Gambar 6.24 Kotak dialog *Save As*

11. Sekembalinya Anda pada kotak dialog *Certificate Export Wizard* maka path penyimpanan file akan muncul, lanjutkan dengan mengklik tombol **Next**.



Gambar 6.25 Path lokasi file *key*

12. Kini proses pembuatan file sertifikat telah selesai dilakukan, klik tombol **Finish**.



Gambar 6.26 Informasi sertifikat

13. Terakhir akan muncul informasi, proses eksport sukses. Klik saja tombol **OK**.



Gambar 6.27 Export sukses

14. Setelah kembali pada kotak dialog *Certificates*, klik saja tombol **Close**. Dan klik tombol **OK** pada kotak dialog *Internet Properties*.

Selamat, Anda telah berhasil membuat file backup untuk kunci (*key*) enkripsi. Sekarang mari kita tengok folder lokasi penyimpanan file *key* yang telah kita buat. Terdapat sebuah file baru dengan nama “kunciku” sesuai dengan nama file yang saya buat sebelumnya.



Gambar 6.28 File key

Salinlah file tersebut ke dalam media lain supaya aman, seperti CD atau flashdisk. Perlu diketahui bahwa, apabila dalam komputer Anda terdapat beberapa account dan seandainya pula setiap account membuat EFS maka masing-masing account harus memiliki file *key* tersendiri. Jadi, satu file *key* tidak bisa digunakan oleh account lainnya.

Sebagai tambahan informasi untuk Anda, berikut saya jelaskan masing-masing file format dari sertifikat yang digunakan:

➤ **Personal Information Exchange (PKCS #12)**

Format *Personal Information Exchange* (PFX, juga disebut PKCS #12) mengaktifkan transfer sertifikat dan hal-hal yang berhubungan dengan *private key* dari satu komputer ke komputer lain, atau dari komputer ke media *removable* seperti flashdisk. Format PKCS #12 adalah satu-satunya format yang didukung oleh Windows 8 untuk mengekspor sertifikat dan hal-hal yang berhubungan dengannya.

➤ **Cryptographic Message Syntax Standard (PKCS #7)**

Format PKCS #7 mengaktifkan transfer sertifikat dan semua sertifikat lainnya yang berada dalam path sertifikat tersebut dari satu komputer ke komputer lain atau dari komputer ke media removable.

➤ **DER Encoded Binary X.509**

Distinguished Encoding Rules (DER) untuk ASN.1, seperti yang dijelaskan dalam ITU-T Recommendation X.509. DER mendukung interoperabilitas antar sistem operasi dan menggunakan ekstensi *.cer.

➤ **Base64 Encoded X.509**

Ini adalah metode encoding yang dikembangkan untuk digunakan dengan Secure/Multipurpose Internet Mail Extensions (S/MIME). Umumnya standar ini digunakan untuk mentransfer attachment dalam bentuk biner via internet. Ekstensi dari sertifikat Base64 adalah *.cer.

6.4 Menggunakan Key Enkripsi

Entah apa gerangan yang terjadi, tiba-tiba saja file-file Anda yang dienkripsi menjadi error sehingga tidak bisa dibuka. Inilah saatnya bagi kita untuk menggunakan *key* yang telah dibuat.

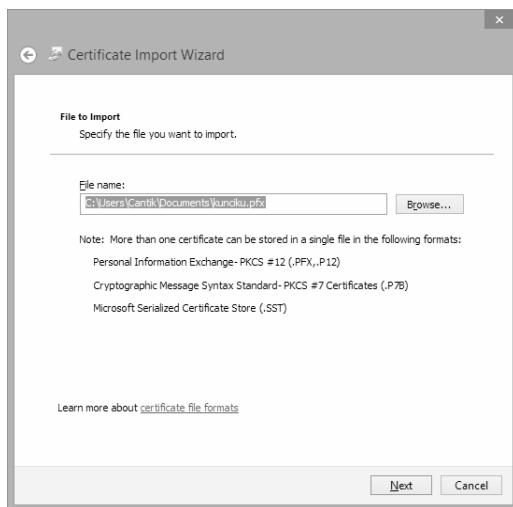
Baiklah langsung saja, ikuti langkah berikut untuk menggunakannya:

1. Jalankan atau klik dua kali pada file *key* yang telah kita buat. Dalam kotak dialog pertama yang tampil, pilihlah **Current User** lalu klik tombol **Next**.



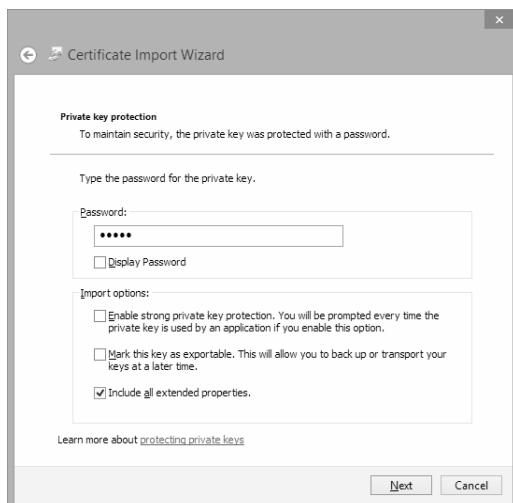
Gambar 6.29 Tampilan Welcome

2. Pada pilihan berikutnya, pastikan path pada bagian *File name* untuk file *key* adalah benar. Apabila Anda tidak sengaja menghapus isian yang ada maka Anda bisa menggunakan tombol *Browse* untuk mencari file *key* secara manual. Kita anggap lokasi file sudah benar lalu klik tombol **Next**.



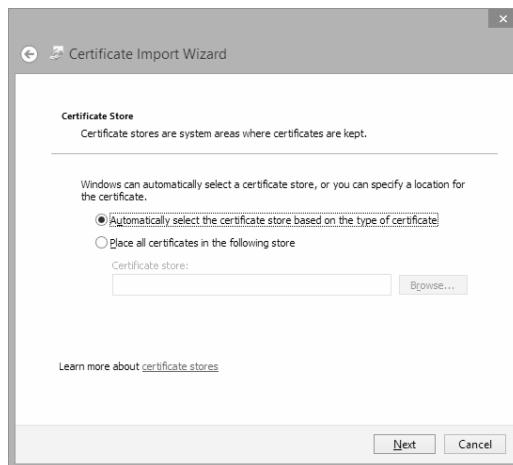
Gambar 6.30 Lokasi file

3. Masukkanlah password yang telah Anda buat sebelumnya. Jika Anda lupa dengan password ini maka maaf sekali, hubungan Anda dengan file tersebut akan berakhir sampai di sini. Semoga Anda masih ingat dengan password-nya lalu klik tombol **Next**.



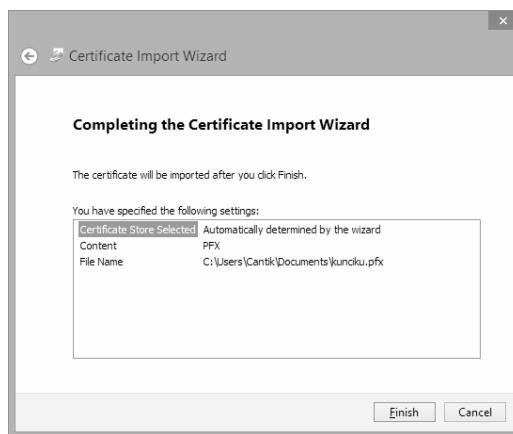
Gambar 6.31 Memasukkan password

4. Berikutnya adalah proses penyimpanan sertifikat akan tampil, dan biarkan program yang memilihnya secara otomatis untuk kita. Klik **Next**.



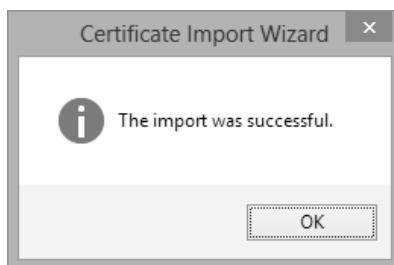
Gambar 6.32 Mencari file sertifikat

5. Terakhir akan ditampilkan informasi mengenai sertifikat yang akan di-import, klik tombol **Finish**.



Gambar 6.33 Informasi sertifikat

6. Apabila semuanya berjalan dengan lancar maka akan tampil informasi bahwa proses import berhasil dilakukan, klik **OK**. Kini file Anda sudah bisa diakses kembali.

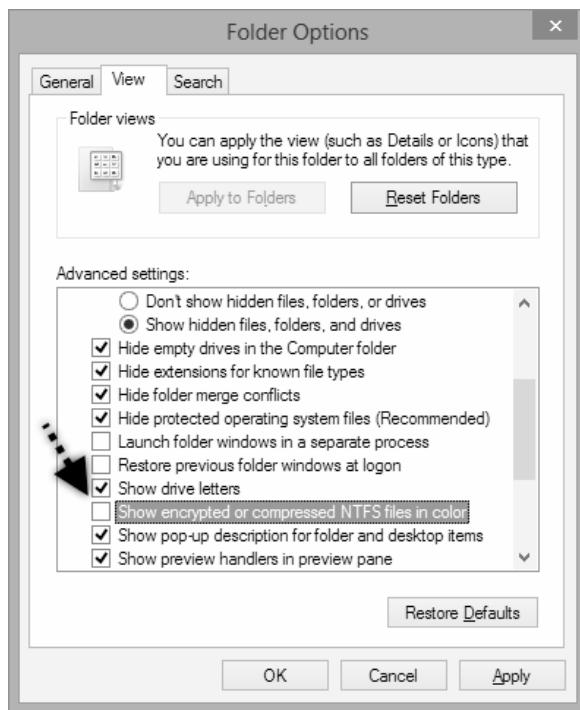


Gambar 6.34 Proses impor sukses

6.5 Tips

Jika Anda perhatikan, terdapat perbedaan yang mencolok antara folder yang dienkripsi (warna hijau) dan yang tidak (warna hitam). Dengan demikian orang lain bisa mengetahui dengan mudah, apakah file tersebut dalam kondisi di enkripsi atau bukan. Berikut adalah tips supaya file yang di-enkripsi tidak menggunakan warna hijau, melainkan tetap berwarna hitam untuk mengelabui orang lain supaya tidak mengetahui bahwa file tersebut dalam keadaan di-enkripsi.

Untuk melakukan hal ini, masuklah ke dalam Control Panel, dan jalankan **Folder Options**. Dalam kotak dialog *Folder Options* yang tampil, klik pada tab **View**. Lalu pada pilihan *Advanced settings*, carilah tulisan **Show encrypted or compressed NTFS files in color**. Hilangkan tanda centang pada bagian tersebut.



Gambar 6.35 Folder Options

Setelah selesai klik tombol **OK**. Dan Anda bisa melihat hasilnya dengan membuka Windows Explorer dan melihat warna teks pada file atau folder yang di-enkripsi kini telah berubah warna menjadi hitam, layaknya file normal lainnya.

7

WINDOWS DEFENDER

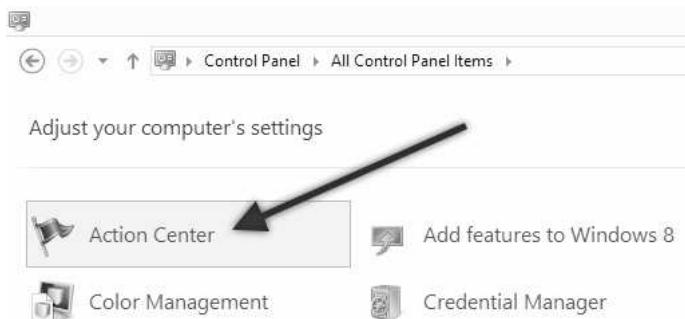
Windows Defender merupakan program bawaan Windows 8 yang berguna untuk melindungi komputer Anda dari *malware* atau program perusak lainnya, seperti virus, spyware dan sebagainya. Boleh dibilang, Windows Defender merupakan program anti virus keluaran Microsoft.

Umumnya apabila dalam komputer Anda sudah terpasang Anti Virus dari pihak ketiga maka Windows Defender akan dinonaktifkan. Masalahnya, banyak yang komputer belum terinstall antivirus tapi Windows Defender-nya juga tidak aktif, sehingga hal ini membahayakan keselamatan komputer Anda.



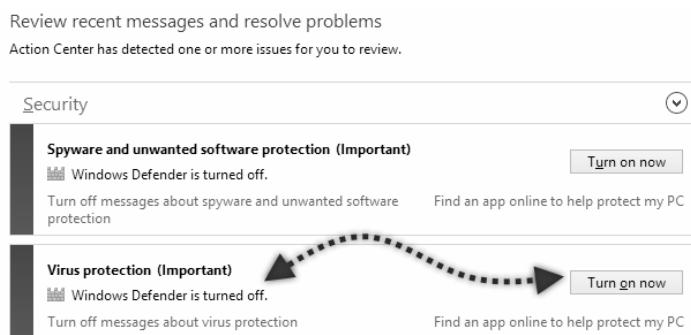
Gambar 7.1 Windows Defender tidak aktif

Untuk mengaktifkan Windows Defender maka Anda harus membuka *Action Center* dari Control Panel.



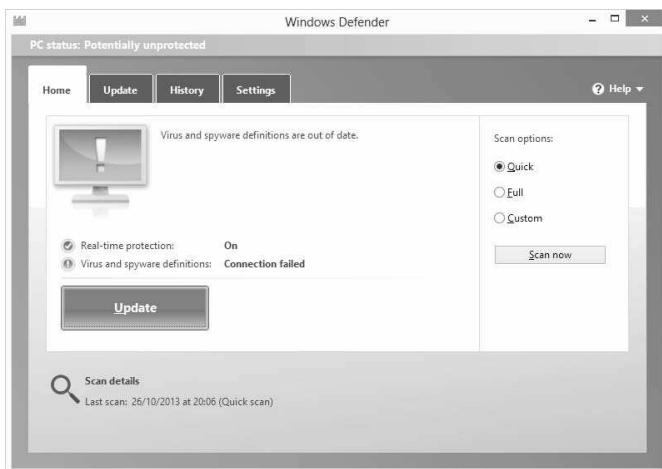
Gambar 7.2 Action Center

Setelah halaman utama *Action Center* tampil, perhatikan pada bagian *Security* yang tertulis *Windows Defender is turned off*. Untuk mengaktifkan Windows Defender klik tombol **Turn on now**.



Gambar 7.3 Mengaktifkan Windows Defender

Secara otomatis maka tampilan utama Windows Defender akan tampil.



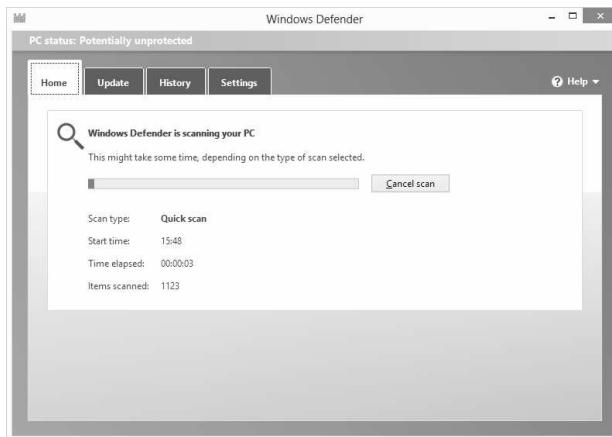
Gambar 7.4 Windows Defender

7.1 Scan Malware

Proses pemeriksaan komputer dari program yang berbahaya (*malware*), lebih dikenal dengan istilah *scan*. Terdapat tiga pilihan model scan yang disediakan oleh Windows Defender:

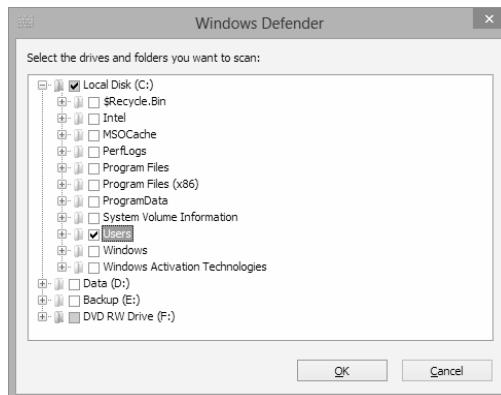
- *Quick*: proses pemeriksaan dengan mode *quick* akan berjalan cepat namun tingkat ketelitiannya rendah.
- *Full*: proses pemeriksaan dilakukan secara menyeluruh dan dengan tingkat ketelitian yang tinggi sehingga proses scan berlangsung lama.
- *Custom*: pilihan ini memberikan keleluasaan kepada user untuk mengatur model scan yang digunakan, serta memilih drive atau folder yang akan di-scan (diperiksa).

Apabila Anda ingin memeriksa keberadaan virus atau *malware* lainnya maka Anda bisa mengklik tombol **Scan now**. Selanjutnya, Anda hanya perlu menunggu proses scanning dilakukan hingga selesai.



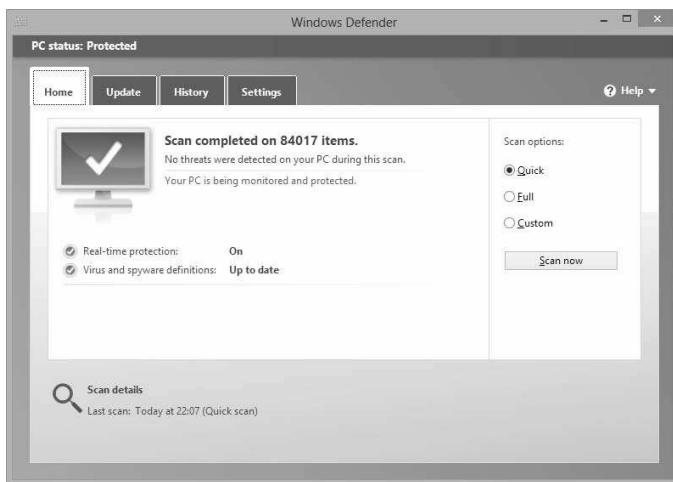
Gambar 7.5 Proses scan

Seandainya Anda memilih model scanning *custom* maka akan muncul sebuah kotak dialog baru yang meminta kita untuk memilih drive atau folder yang akan di-scan. Setelah Anda menentukan drive atau folder yang akan discan, dan mengklik *OK* barulah proses scan dilakukan.



Gambar 7.6 Mencari Folder

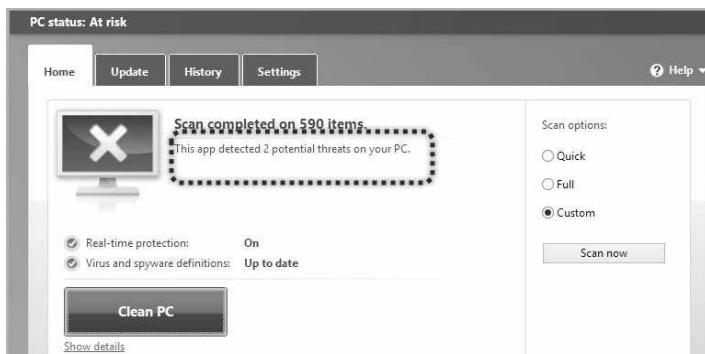
Setelah proses scanning selesai maka akan tampil informasi hasil pemeriksaan. Dari gambar di bawah ini dilaporkan terdapat 84.017 item yang sudah diperiksa, serta tidak ditemukan keberadaan program berbahaya dalam komputer sewaktu pemeriksaan tersebut berlangsung.



Gambar 7.7 Scan selesai

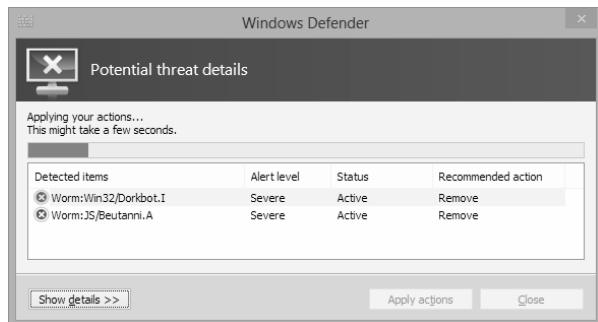
Berikut adalah contoh lainnya, di mana komputer menemukan virus dalam flashdisk yang saya scan. Dari gambar di bawah ini terlihat bahwa Windows Defender menemukan 2 ancaman dari virus. Selain itu, dari *PC status*, terdapat pesan *At risk* yang berarti komputer Anda berisiko.

Dan untuk membasmi virus ataupun *malware* tersebut, klik tombol **Clean PC**.



Gambar 7.8 Terdeteksi malware

Kemudian tunggu lah proses pembersihan dilakukan sampai selesai.



Gambar 7.9 Proses pembersihan

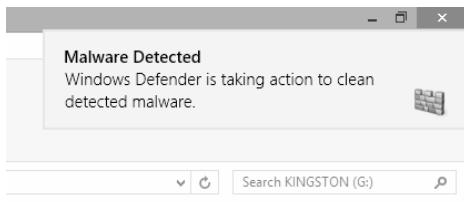
Setelah proses pembersihan selesai maka perhatikan pada kolom status yang bertuliskan *Succeeded* yang berarti virus berhasil dilumpuhkan. Terakhir klik tombol **Close** untuk menutup halaman tersebut.



Gambar 7.10 Pembersihan berhasil

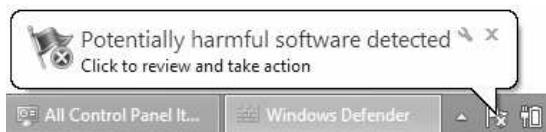
7.2 Real-time Protection

Apabila fitur *Real time protection* dalam kondisi aktif maka Windows Defender dapat mendeteksi keberadaan virus secara *real time*. Sebagai contoh, pada saat kita memasukkan sebuah flashdisk yang mengandung virus maka pada layar komputer muncul pesan peringatan: *Malware Detected*. Secara otomatis Windows Defender langsung menerapkan tindakan pencegahan dan menginformasikannya kepada Anda.



Gambar 7.11 Terdeteksi malware

Selain tampilan seperti di atas, terkadang pada bagian *systray* Windows muncul pesan *Potentially harmful software detected*. Hal ini berarti ada program berbahaya yang menyerang komputer Anda.



Gambar 7.12 Ditemukan program berbahaya

Oleh karena itulah fasilitas *Real-time protection* ini sebaiknya selalu Anda aktifkan.

7.3 Melihat Hasil Temuan Windows Defender

Terkadang sewaktu Anda menjalankan Windows Defender terdapat informasi *This app detected a potential threat on your PC*. Hal ini menandakan adanya program yang dianggap berbahaya oleh Windows Defender. Jika Anda ingin mengetahui file apakah yang dianggap berbahaya tersebut maka Anda bisa klik link **Show details**.



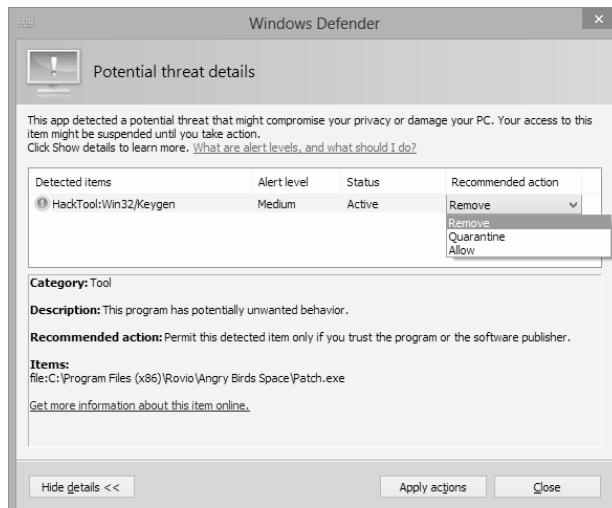
Gambar 7.13 Show details

Berikutnya akan tampil informasi mengenai program yang dicurigai tersebut.



Gambar 7.14 *Informasi malware*

Jika Anda ingin mengetahui di mana tepatnya lokasi file tersebut, klik tombol **Show details >>**. Dari gambar di bawah ini terlihat bahwa program tersebut merupakan patch dari game Angry Bird dalam komputer saya.



Gambar 7.15 *Memilih tindakan*

Penanganan setiap program yang mencurigakan terdapat tiga jenis:

- *Remove*: maka file yang dimaksud akan dihapus dari dalam komputer.
- *Quarantine*: file yang dianggap berbahaya tersebut akan dimasukkan dalam lokasi sendiri dan tidak bisa digunakan, alias dipenjara.
- *Allow*: apabila Anda yakin serta percaya bahwa file tersebut tidak berbahaya maka Anda bisa memilih pilihan ini yang berarti mengizinkannya untuk tetap aktif.

Setelah Anda menentukan salah satu tindakan yang akan Anda ambil, klik tombol **Apply actions**. Sebagai contoh di sini, saya akan mengkarantina file yang ditemukan tersebut. Tunggu lah proses dilakukan hingga selesai.

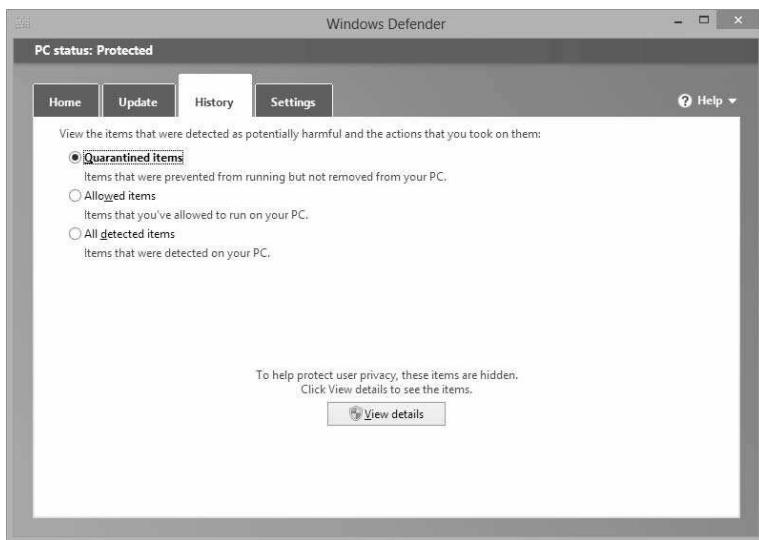
Jika semuanya berjalan lancar maka akan tampil pesan *Your actions were applied successfully*.



Gambar 7.16 Tindakan berhasil dilakukan

Terakhir klik tombol **Close** untuk keluar dari kotak dialog tersebut.

Setelah Anda mengetahui cara melihat hasil temuan Windows Defender, lebih tepatnya *malware* apa yang menyerang komputer. Kita juga bisa melihat history atau catatan temuan yang pernah dilakukan oleh Windows Defender. Hal ini bisa Anda lihat dalam tab *History*.



Gambar 7.17 Tab History

Dalam tab *History* tersebut terdapat tiga pilihan yang bisa Anda pilih:

- *Quarantined items*: menunjukkan item atau *malware* yang sedang dikarantina oleh Windows Defender.
- *Allowed items*: menunjukkan item yang dianggap berbahaya oleh Windows Defender tapi Anda tetap mengizinkan program tersebut aktif.
- *All detected items*: menampilkan semua *malware* yang pernah terdeteksi oleh Windows Defender baik berbahaya atau tidak.

Sebagai contoh saya, akan melihat semua *malware* yang pernah terdeteksi oleh Windows Defender dalam komputer saya. Berikan pilihan pada bagian **All detected items**, lalu klik tombol **View details**.

Selanjutnya akan ditampilkan virus dan sejenisnya yang pernah dideteksi oleh Windows Defender. Pada kolom *Action taken* menunjukkan jenis tindakan yang pernah diambil oleh Windows Defender, ada yang dihapus (*Removed*), ada pula yang di karantina (*Quarantined*).

Dan pada bagian bawahnya terdapat informasi mengenai *malware* tersebut, misalnya tergolong malware jenis apa, disertai penjelasan singkat.

The screenshot shows the Windows Defender application window. At the top, there are tabs: Home, Update, History, Settings, and Help. The 'Settings' tab is selected. Below the tabs, a message says: "View the items that were detected as potentially harmful and the actions that you took on them:". There are three radio button options: "Quarantined items", "Allowed items", and "All detected items". The "All detected items" option is selected. A note below it says: "Items that were detected on your PC." Below this, a table lists detected items:

Detected item	Alert level	Date	Action taken
<input type="checkbox"/> Worm:S/Beutanni.A	Severe	19/10/2014 16:49	Removed
<input type="checkbox"/> Worm:Win32/Dorkbot.l	Severe	19/10/2014 16:49	Removed
<input type="checkbox"/> Worm:Win32/Dorkbot.l	Severe	19/10/2014 16:41	Quarantined
<input type="checkbox"/> HackTool:Win32/Keygen	Medium	19/10/2014 12:29	Quarantined

Below the table, there is a section titled "Category: Worm" with a description: "Description: This program is dangerous and self-propagates over a network connection." and a recommended action: "Recommended action: Remove this software immediately." At the bottom right are two buttons: "Remove all" and "Allow item".

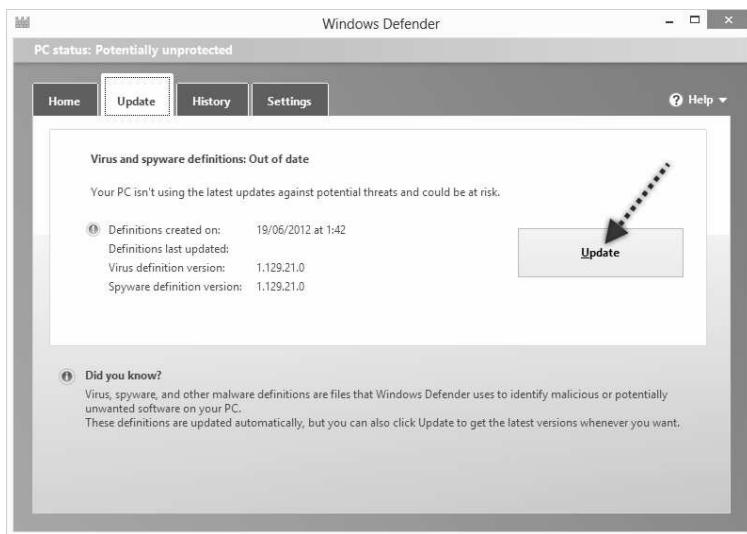
Gambar 7.18 Melihat item yang pernah ditemukan

Apabila Anda ingin menghapus semua isi pada daftar tersebut, klik tombol **Remove all**.

7.4 Update Windows Defender

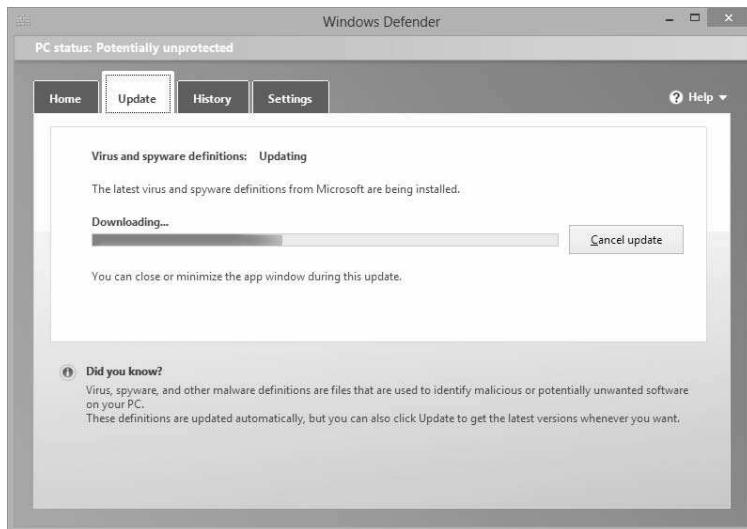
Seiring dengan semakin berkembangnya virus dan juga varian-nya maka sangat penting bagi kita untuk sering-sering melakukan update terhadap program ini. Terutama sekali apabila informasi yang ditampilkan dalam tab *Update: Virus and spyware definitions: Out of date*. Hal ini menunjukkan definisi virus Windows Defender telah kadaluarsa.

Untuk melakukan update, pastikan Anda terhubung ke internet. Lalu dalam tab *Update* klik tombol **Update**.



Gambar 7.19 Tab Update

Selanjutnya tunggu lah proses update dilakukan sampai selesai.



Gambar 7.20 Proses update

Apabila proses update Windows berhasil dilakukan maka pada tab *Update* akan tampil informasi *Virus and spyware definitions: up to date*.

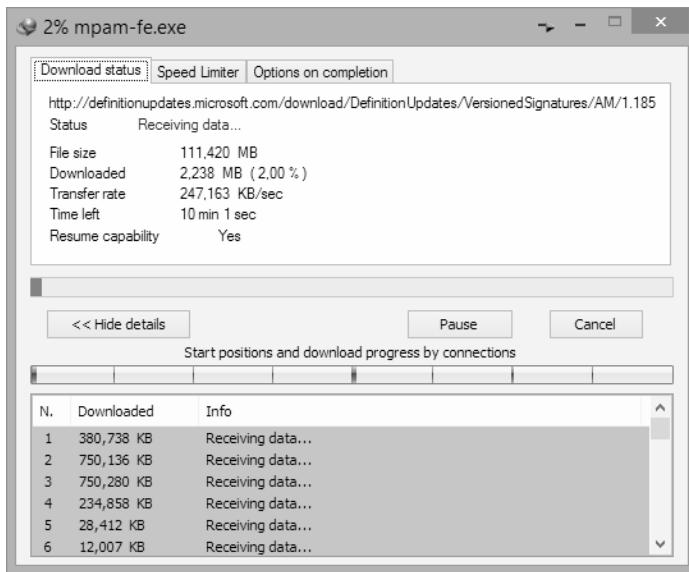
Manakala proses update dengan cara di atas berjalan tidak lancar maka Anda bisa melakukan update Windows Defender dengan mendownload langsung file *virus definiton* dan menginstallnya dalam komputer. Untuk melakukan hal ini, bukalah website pada alamat berikut: <http://www.microsoft.com/security/portal/definitions/adl.aspx>

Geserlah halaman website ke bawah dan carilah versi Windows yang Anda gunakan, yang dalam hal ini adalah Windows 8. Tentukan pula berapa bit versi Windows Anda, apakah 32 bit atau 64 bit. Jika Anda tidak tahu pasti berapa bit Windows 8 yang Anda gunakan, silahkan baca bab terakhir dalam buku ini, tepatnya pada subbab Mencari Versi Windows. Setelah Anda yakin, barulah klik link tersebut.



Gambar 7.21 Download update Windows Defender

Maka proses download file *virus definition* segera dilakukan.

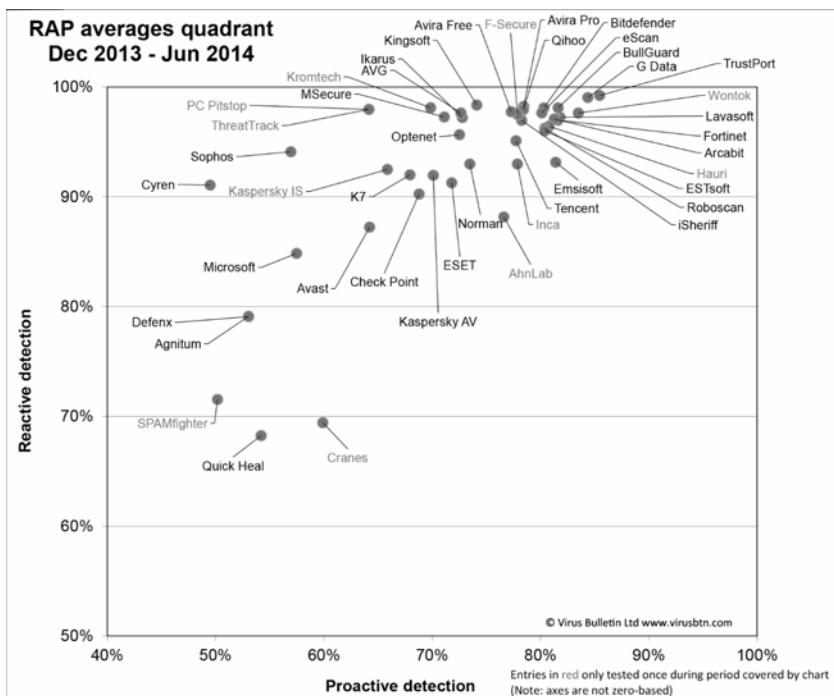


Gambar 7.22 Proses download

Setelah download berhasil dilakukan Anda hanya perlu menginstall file yang telah Anda download tersebut.

7.5 Tips

Sejauh ini pemakaian Windows Defender tidak begitu maksimal karena ada banyak program Anti Virus lain yang beredar dengan kemampuan deteksi yang lebih baik. Untuk mengetahui kemampuan deteksi dan proteksi terhadap *malware* bisa kita lihat dari RAP (*Reactive And Proactive*) Quadrant yang dikeluarkan oleh Virus Bulletin. Berikut adalah gambar RAP dari Desember 2013 sampai dengan Juni 2014.



Gambar 7.23 RAP Quadrant

Untuk memperkuat sistem keamanan terhadap virus ini, pada beberapa kasus Windows Defender bisa digabung dengan beberapa antivirus lain. Oleh karena itu, apabila Anda memasang dua pertahanan sekaligus terhadap virus maka daya tahan komputer Anda bisa meningkat. Dan satu hal yang penting, yaitu sering-seringlah melakukan update Windows Defender Anda, supaya memiliki definisi virus terbaru. Dengan demikian apabila ada virus baru yang menyerang komputer Anda menjadi tidak berikutik.

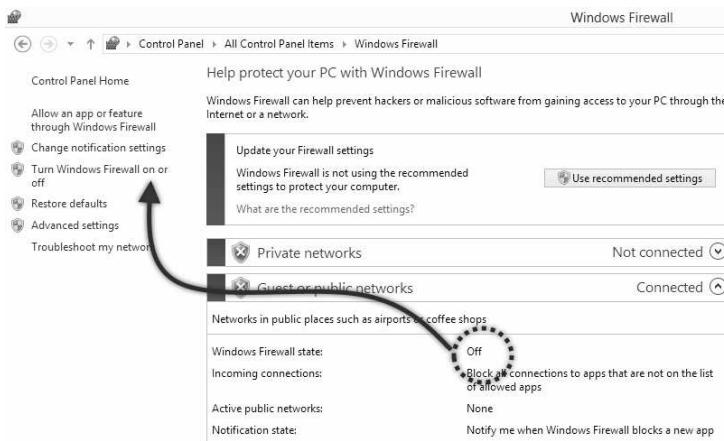
Sebagai tips tambahan berikutnya, hindarilah untuk mengklik sembarang tombol download sewaktu Anda mengunjungi sebuah website. Sebab, ada banyak virus, spyware, worm dan sebagai berasal dari internet. Jika memang Anda ingin mendownload atau menginstall sebuah program pastikan tempat Anda mendownloadnya berasal dari sumber terpercaya serta bacalah *license agreement* terlebih dahulu jangan asal klik *Next*.

8

WINDOWS FIREWALL

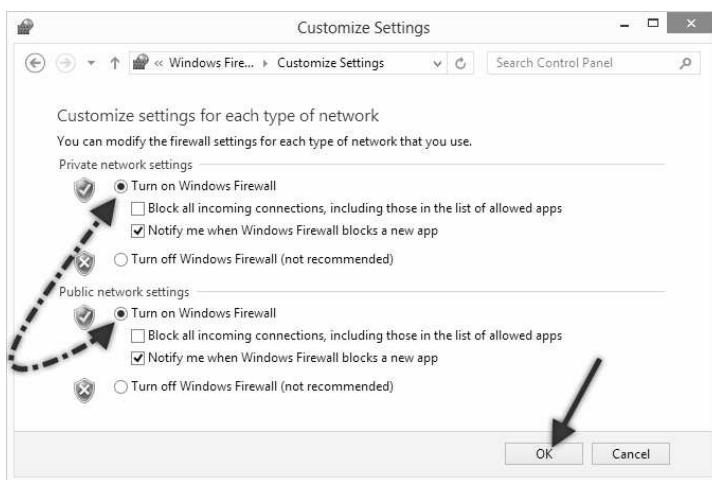
Windows Firewall berfungsi untuk mencegah serangan dari program yang berbahaya ataupun dari aksi cracker yang berasal dari jaringan atau internet, yang umumnya bertujuan untuk mengakses komputer kita. Sebaliknya dengan adanya firewall juga akan mencegah terjadinya pengiriman program yang berbahaya dari komputer kita ke komputer lain dalam sebuah jaringan maupun internet.

Untuk menjalankan program ini Anda hanya perlu mengklik ikon **Windows Firewall** dalam Control Panel. Tindakan pertama yang harus Anda ambil, adalah mencari tahu apakah Windows Firewall yang Anda gunakan sedang aktif atau tidak. Apabila tidak maka Anda bisa mengaktifkannya dengan mengklik link **Turn Windows Firewall on or off** yang berada pada panel sebelah kiri.



Gambar 8.1 Status Windows Firewall

Dari tampilan berikutnya, gunakan pilihan pada **Turn on Windows Firewall**, baik pada bagian *Private network settings* maupun pada *Public network settings*.



Gambar 8.2 Mengaktifkan Windows Firewall

Setelah selesai, klik tombol **OK**. Kini status Windows Firewall telah menjadi *On*.



Gambar 8.3 Windows Firewall aktif

8.1 Mengatur Program Melalui Firewall

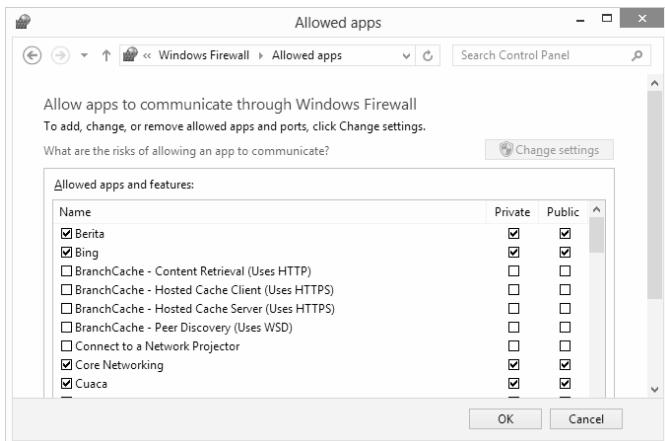
Penggunaan firewall banyak berhubungan dengan akses jaringan dan internet. Firewall juga akan memonitor komunikasi yang terjadi dalam komputer kita. Ada dua cara untuk mengatur program melalui firewall:

- Menambahkan program pada daftar program. Cara ini dapat mengurangi resiko keamanan.
- Membuka sebuah port. Cara ini sangat risikan dari sisi keamanan.

Dengan fitur ini maka kita bisa menentukan program apa saja yang boleh berjalan dan program apa saja yang tidak boleh berjalan. Untuk meningkatkan keamanan komputer Anda maka izinkan hanya program yang benar-benar Anda perlukan saja yang bisa terhubung ke internet. Dan hindarilah untuk mengizinkan program yang tidak Anda kenal untuk berkomunikasi melalui firewall.

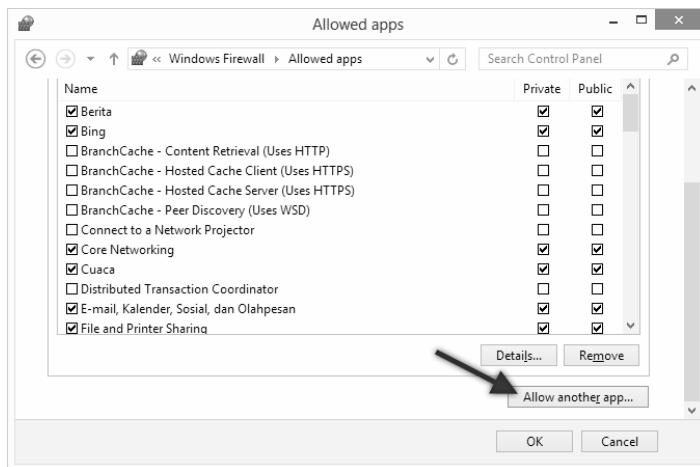
Untuk menambah atau menghapus daftar program dari firewall adalah sebagai berikut:

1. Bukalah Windows Firewall terlebih dahulu.
2. Pada panel sebelah kiri, klik pada Allow an app or feature through Windows Firewall.
3. Dari tampilan berikutnya, berilah tanda centang pada nama program yang Anda izinkan berkomunikasi melalui firewall.
4. Selanjutnya, berikan tanda centang pada bagian *Private* yang berarti untuk jaringan yang bisa Anda percaya misalnya dari modem Anda pribadi. Sedangkan *Public* berarti jenis jaringan pada lokasi umum, misalnya WiFi gratis di mall atau hotel.



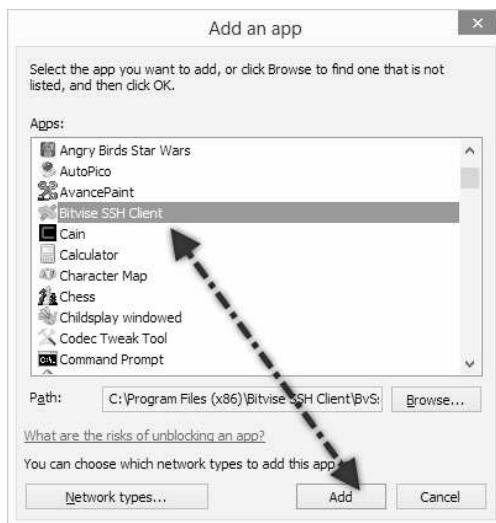
Gambar 8.4 Aplikasi yang diizinkan

5. Setelah Anda menentukan program yang bisa atau tidak melalui Windows Firewall, klik tombol **OK**.
6. Sebagai tambahan, apabila Anda ingin menambahkan program lainnya yang tidak terdapat pada daftar program maka klik tombol **Allow another app...** yang terdapat pada bagian bawah.



Gambar 8.5 Memilih aplikasi lain

7. Lanjutkan dengan mencari nama program yang terdapat dalam komputer Anda. Atau bisa juga dengan menekan tombol *Browse* untuk mencari program secara manual.
8. Setelah program yang Anda cari ditemukan, klik pada program tersebut lalu klik tombol **Add**.



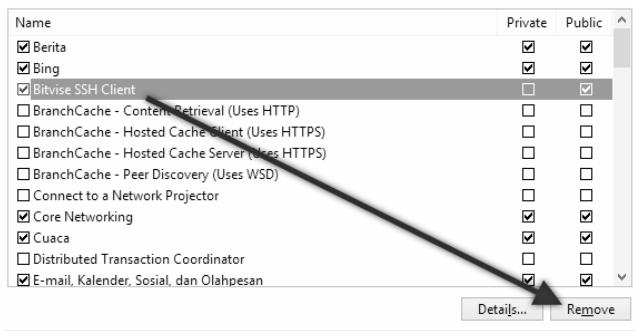
Gambar 8.6 Memilih aplikasi

Sekarang program yang Anda pilih telah masuk dalam daftar program Firewall. Terakhir jangan lupa klik tombol **OK**.

Name	Private	Public
<input checked="" type="checkbox"/> Berita	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/> Bing	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/> Bitvise SSH Client	<input type="checkbox"/>	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/> BranchCache - Content Replication (Uses HTTPS)	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/> BranchCache - Hosted Cache Client (Uses HTTPS)	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> BranchCache - Hosted Cache Server (Uses HTTPS)	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> BranchCache - Peer Discovery (Uses WSD)	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> Connect to a Network Projector	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/> Core Networking	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/> Cuaca	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/> Distributed Transaction Coordinator	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/> E-mail, Kalender, Sosial, dan Olahpesan	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

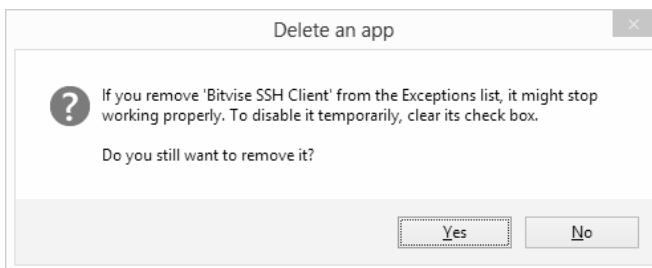
Gambar 8.7 Aplikasi yang diizinkan

Sebaliknya, jika Anda ingin menghapus program dari daftar firewall maka Anda hanya perlu memilih program tersebut lalu klik tombol **Remove**.



Gambar 8.8 Menghapus aplikasi dari daftar

Jika muncul kotak dialog konfirmasi, apakah Anda yakin akan menghapus program tersebut dari daftar, klik **Yes**.



Gambar 8.9 Konfirmasi penghapusan

8.2 Windows Firewall with Advanced Security

Sekarang kita akan melakukan beberapa pengaturan lebih lanjut dalam mengelola firewall. Untuk membuka *Windows Firewall with Advanced Security*, dalam halaman utama Windows Firewall, klik pada **Advanced settings** yang berada pada panel sebelah kiri.

Control Panel Home

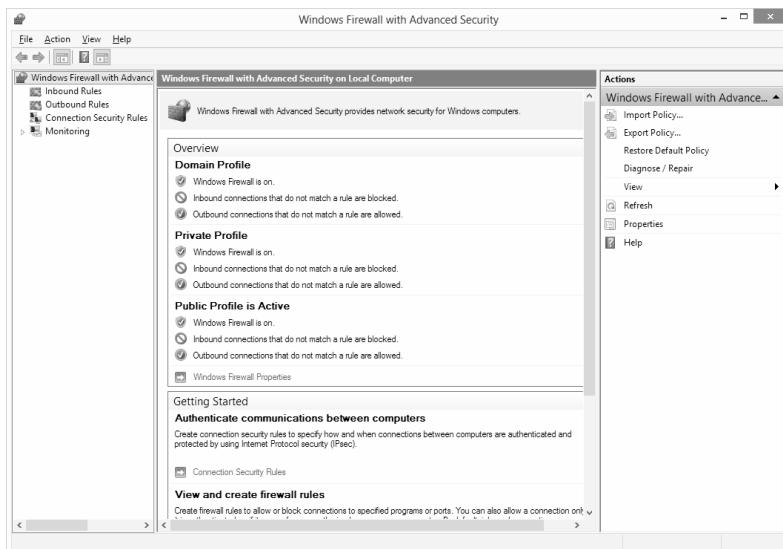
Allow an app or feature through Windows Firewall

- Change notification settings
- Turn Windows Firewall on or off
- Restore defaults
- Advanced settings (arrow pointing to this item)

Troubleshoot my network

Gambar 8.10 Advanced settings

Selanjutnya akan terbuka jendela kerja *Windows Firewall with Advanced Security*.



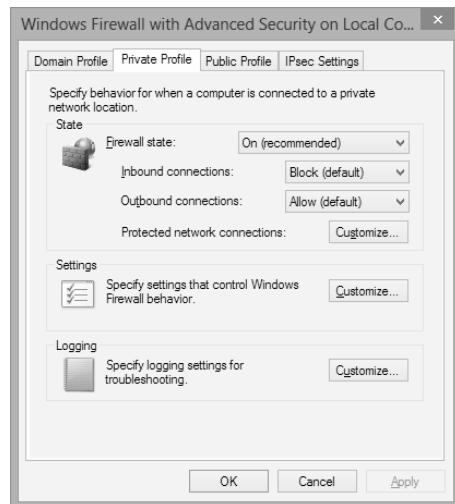
Gambar 8.11 Windows Firewall with Advanced Security

Dari tampilan pertama tersebut kita dapat melihat status firewall pada bagian *Overview*. Pada gambar terlihat bahwa saya telah mengaktifkan (ON) Windows Firewall baik untuk *Domain Profile*, *Private Profile*, dan *Public Profile*.

Dan di bagian bawahnya terdapat link **Windows Firewall Properties**. Klik pada link tersebut maka akan tampil kotak dialog *Windows Firewall with Advanced Security-Local Group Policy Object*. Dalam kotak dialog tersebut terdapat empat tab:

- *Domain Profile*, berfungsi untuk mengatur perilaku Firewall saat terhubung ke suatu Domain dalam jaringan.
- *Private Profile*, berfungsi untuk mengatur perilaku Firewall saat terhubung ke jaringan lokal.
- *Public Profile*, berfungsi untuk mengatur perilaku Firewall saat terhubung ke jaringan publik seperti internet.
- *IPsec Settings*, berfungsi untuk mengatur *IP security* (IPsec) dalam sebuah jaringan yang aman (*secured*).

Setiap tab tersebut memiliki isi yang sama, kecuali tab *IPsec Settings*. Sebagai contoh, kita lihat tab *Private Profile* saja.



Gambar 8.12 Tab Private Profile

Untuk mengaktifkan firewall maka kita atur setting *Firewall state* menjadi **On (recommended)**.

Untuk *Inbound Connections* (koneksi masuk) dan *Outbound Connections* (koneksi keluar), dapat diatur melalui *dropdown list*, yaitu:

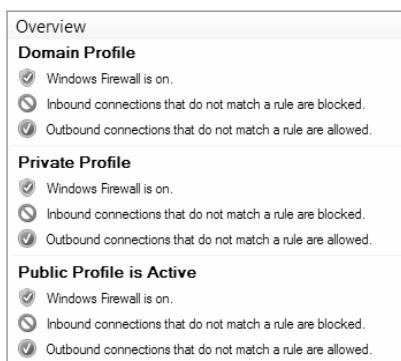
- *Block*, digunakan untuk memblok data yang masuk (*inbound*) atau keluar (*inbound*).
- *Allow*, digunakan untuk mengizinkan data masuk (*inbound*) atau keluar (*inbound*)
- *Block all connections*, digunakan untuk memblok semua koneksi yang terjadi. Pilihan ini hanya terdapat pada bagian *inbound*.

Silahkan Anda atur sesuai dengan pengaturan yang diinginkan, namun jika Anda tidak paham sebaiknya pilih saja yang ada kata *default*. Karena itu adalah setting dasar yang disediakan oleh Windows.

Untuk pengaturan bagian *Settings* dan *Logging* tidak saya bahas terlalu mendalam karena *Settings* digunakan hanya untuk mengatur perilaku dari Windows Firewall. Sedangkan *Logging* berguna untuk mengatur log atau pencatatan.

8.3 Inbound & Outbound Rules

Setelah mengatur baik *Inbound Rules* dan *Outbound Rules* seperti yang telah dijelaskan sebelumnya. Jika ada perubahan maka pada bagian *Overview* jendela kerja *Windows Firewall with Advanced Security* akan ditampilkan hasilnya.

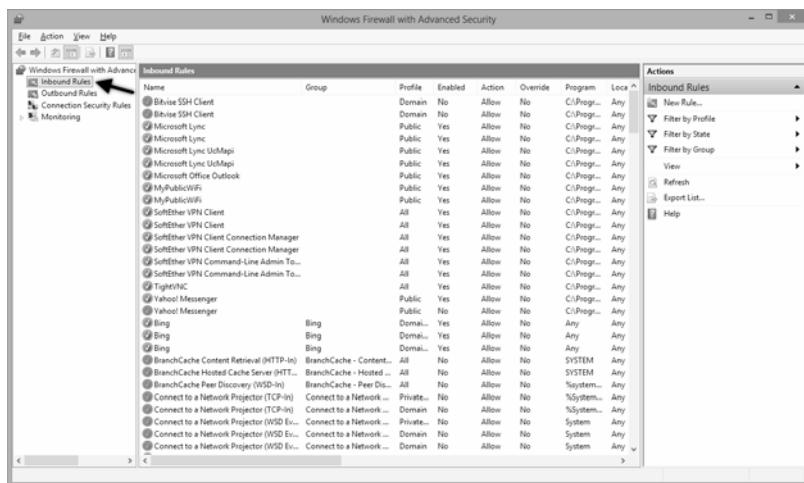


Gambar 8.13 Informasi inbound dan outbound

Dari gambar di atas terlihat bahwa saya mengatur *Inbound*, baik pada *Domain Profile*, *Private Profile*, dan *Public Profile is Active*, semuanya

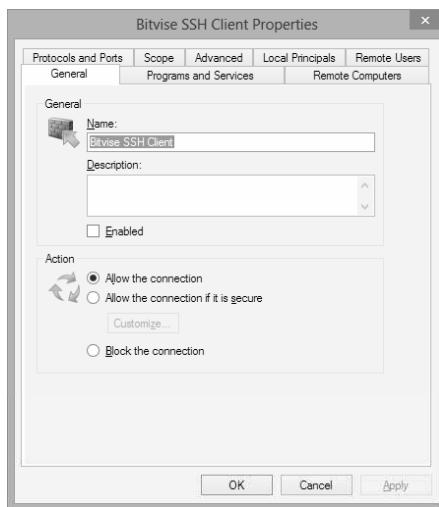
saya atur sesuai default dengan memilih *Block*. Sedangkan untuk *Outbound* di aktifkan (*allowed*).

Sekarang klik pilihan **Inbound Rules** yang berada pada panel sebelah kiri. Maka pada bagian sebelah kanan akan tampil pengaturan koneksi *Inbound*. Kolom *Name* menunjukkan nama programnya, sedangkan kolom berikutnya menunjukkan status dan juga aturan (*Rules*) mengenai program tersebut.



Gambar 8.14 Memilih Inbound Rules

Untuk mengatur perilaku lainnya klik pada salah satu nama program yang Anda inginkan. Maka akan tampil kotak dialog *Properties* dari program yang Anda pilih. Di dalamnya terdapat pula banyak tab yang bisa digunakan untuk pengaturan, di antaranya adalah deskripsi program (jika ada), lokasi file, protokol dan port yang digunakan, dan sebagainya.



Gambar 8.15 Properti program

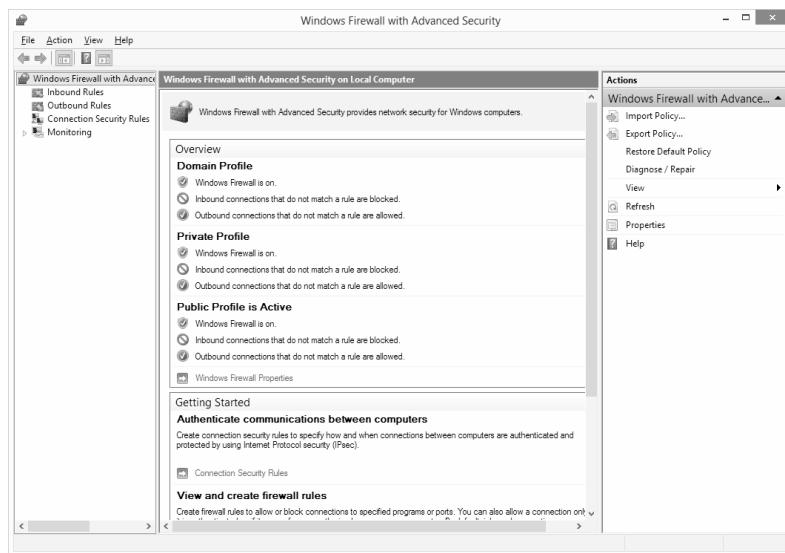
Sebagai contoh, pada tab *General* di bagian *Action* Anda bisa mengatur untuk mengizinkan koneksi. Anda tinggal memilih *Allow the connection*, atau untuk memblokir koneksi dari program tersebut pilihlah *Block the connection*. Sedangkan pilihan *Allow the connection if it secure* pilihan ini digunakan jika Anda yakin bahwa koneksi tersebut aman dan Anda juga bisa mengatur melalui tombol *Customize*. Aturlah dengan bijak, setelah selesai, klik **OK**.

Untuk pengaturan *Outbound Rules*, langkah yang harus dilakukan adalah sama persis seperti *Inbound Rules*. Jadi, saya rasa kita tidak perlu berpanjang lebar lagi.

Sekedar saran dari saya, karena ada banyak *rules*, jika Anda tidak mengetahuinya sebaiknya biarkan saja sesuai dengan default yang ada.

8.4 Menutup Port

Jika Anda ingin menutup port, dari halaman utama Windows Firewall, klik pada **Advanced settings** yang berada pada panel sebelah kiri. Selanjutnya akan terbuka jendela kerja *Windows Firewall with Advanced Security*.



Gambar 8.16 Windows Firewall Advanced Security

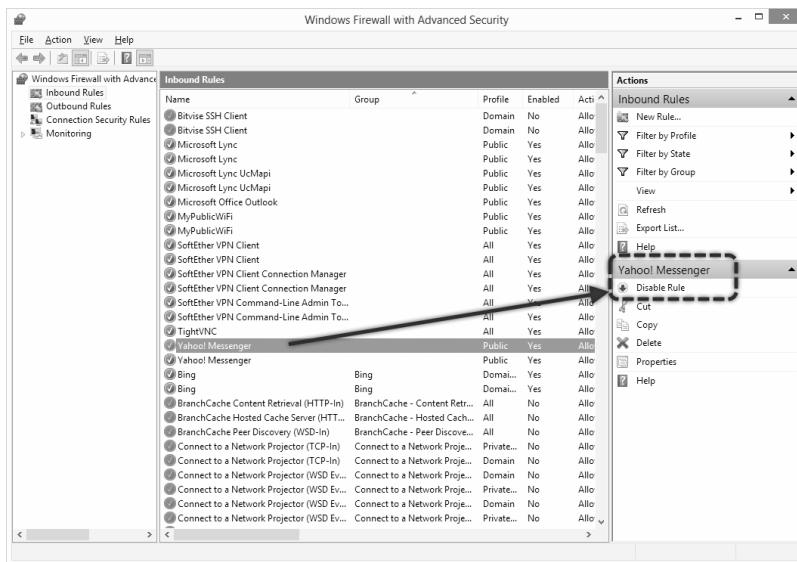
Dari panel sebelah kiri *Windows Firewall with Advanced Security*, klik pada **Inbound Rules**.

The screenshot shows the Windows Firewall with Advanced Security window with the Inbound Rules section selected in the left navigation pane. The main area displays a table of Inbound Rules. The columns are Name, Group, Profile, Enabled, and Action. The table lists numerous rules, including Bitvise SSH Client, Microsoft Lync, Microsoft Office Outlook, MyPublicWiFi, SoftEther VPN Client, and various Microsoft services like Bing, BranchCache, and Connect to a Network Projector. The right side has an Actions pane with options like New Rule..., Filter by State, Filter by Group, View, Refresh, Export List..., and Help.

Name	Group	Profile	Enabled	Action
Bitvise SSH Client		Domain	No	All
Bitvise SSH Client		Domain	No	All
Microsoft Lync		Public	Yes	All
Microsoft Lync		Public	Yes	All
Microsoft Lync UcMapi		Public	Yes	All
Microsoft Lync UcMapi		Public	Yes	All
Microsoft Office Outlook		Public	Yes	All
MyPublicWiFi		Public	Yes	All
MyPublicWiFi		Public	Yes	All
SoftEther VPN Client		All	Yes	All
SoftEther VPN Client		All	Yes	All
SoftEther VPN Client Connection Manager		All	Yes	All
SoftEther VPN Client Connection Manager		All	Yes	All
SoftEther VPN Command-Line Admin To...		All	Yes	All
SoftEther VPN Command-Line Admin To...		All	Yes	All
TightVNC		All	Yes	All
Yahoo! Messenger		Public	Yes	All
Yahoo! Messenger		Public	Yes	All
Bing	Bing	Domai...	Yes	All
Bing	Bing	Domai...	Yes	All
BranchCache Content Retrieval (HTTP-In)	BranchCache - Content Retr...	All	No	All
BranchCache Hosted Cache Server (HTTP...	BranchCache - Hosted Cach...	All	No	All
BranchCache Peer Discovery (WSD-In)	BranchCache - Peer Discove...	All	No	All
Connect to a Network Projector (TCP-In)	Connect to a Network Proj...	Private...	No	All
Connect to a Network Projector (TCP-In)	Connect to a Network Proj...	Domain	No	All
Connect to a Network Projector (WSD ...	Connect to a Network Proj...	Domain	No	All

Gambar 8.17 Inbound Rules

Selanjutnya, perhatikan pada panel yang tengah carilah program yang akan Anda nonaktifkan, lalu klik pada program tersebut. Kemudian menuju pada panel sebelah kanan klik pada **Disable Rule**.



Gambar 8.18 Disable Rule

8.5 Tips

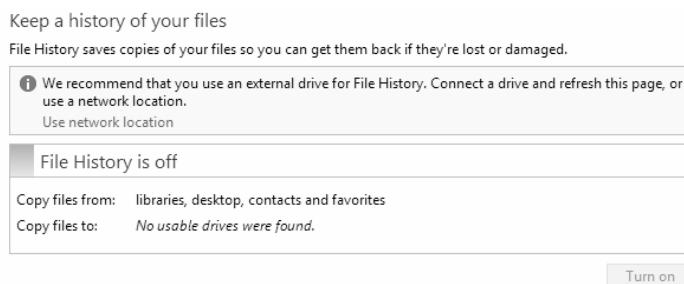
Sewaktu Anda mengakses internet maka mengaktifkan Windows Firewall adalah hal yang wajib dilakukan supaya Anda tidak menjadi korban penularan virus dari pihak luar. Siapa tahu ada program yang diam-diam bersembunyi dalam komputer Anda. Sehingga ketika ada program yang tidak dikenal secara tiba-tiba mengakses internet Anda, maka bisa diketahui dan ditangguangi secepatnya oleh Windows Firewall.

9

FILE HISTORY

File History adalah fitur Windows 8 yang digunakan untuk menyimpan salinan file Anda alias sebagai backup atau cadangan. Sehingga apabila file tersebut hilang atau rusak maka Anda bisa mendapatkannya kembali dengan mudah.

Untuk menjalankan *File History* ini terdapat dalam Control Panel. Berikut tampilannya ketika pertama kali digunakan.



Gambar 9.1 Status File History

Dari gambar di atas, status *File History is off* alias tidak aktif. Sedangkan untuk mengaktifkannya dari tombol *Turn on* juga tidak bisa diklik. Hal ini terjadi karena Anda disarankan untuk menggunakan *eksternal drive* untuk menjalankan *File History*. Jadi Anda bisa menggunakan harddisk eksternal, flashdisk, atau terhubung ke media penyimpanan lain di jaringan.

Sebagai contoh di sini saya menggunakan flashdisk. Setelah flashdisk saya pasang maka status di atas masih belum berubah. Tekan saja tombol **F5** pada keyboard untuk me-refresh. Berikut tampilannya, dan tombol *Turn on* juga segera berubah menjadi aktif.

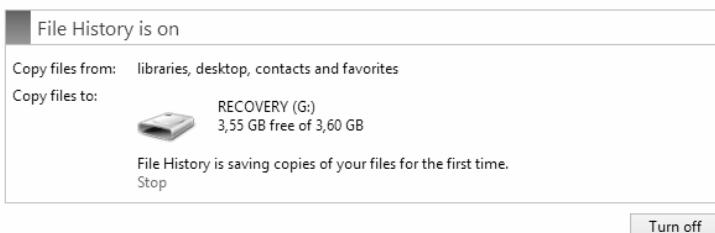
Keep a history of your files

File History saves copies of your files so you can get them back if they're lost or damaged.



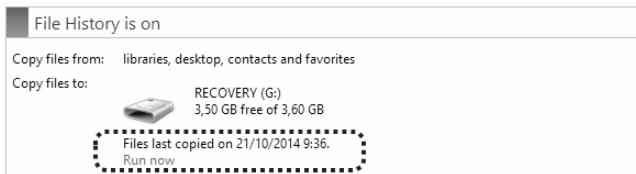
Gambar 9.2 File History tidak aktif

Klik tombol **Turn on** tersebut untuk mengaktifkan *File History* lalu tunggu lah prosesnya beberapa saat. Setelah selesai kini status *File History is on*, alias sudah aktif.



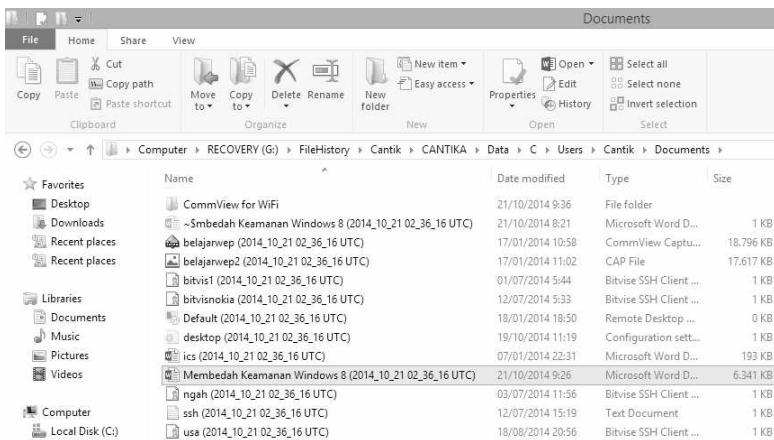
Gambar 9.3 File History aktif

Biasanya, secara otomatis pula *File History* akan menyalin file yang terdapat dalam folder *Libraries*, *desktop*, *contact*, dan *favorites*. Dibackup ke dalam flashdisk Anda. Apabila proses penyalinan file telah selesai dilakukan maka link *Stop* berubah menjadi *Run now*. Fungsinya adalah untuk melakukan penyalinan ulang jika diperlukan.



Gambar 9.4 Informasi penyalinan terakhir

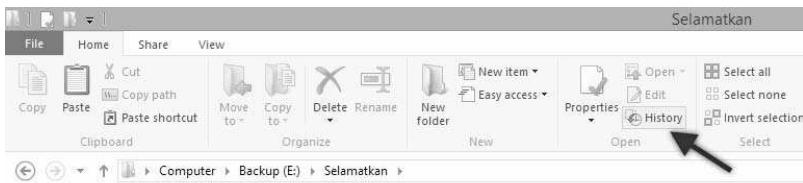
Selain itu, jika membuka Anda flashdisk maka akan terdapat sebuah folder yang bernama FileHistory. Di dalamnya, Anda bisa melihat berbagai file yang disalin. Sebagai contoh seperti gambar di bawah ini, semua file dalam folder Documents disalin semuanya. Bedanya, pada nama file akan disertai dengan tanggal penyalinan.



Gambar 9.5 File Backup

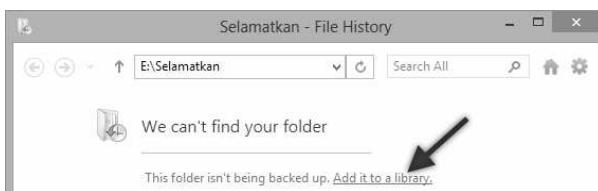
9.1 Membbackup Data

Sekarang, pertanyaannya bagaimana cara kita membackup file atau folder lainnya, selain folder default di atas. Caranya adalah dengan membuka File Explorer (Windows Explorer). Lalu carilah folder yang akan Anda buat backup-nya. Sebagai contoh, saya akan mem-backup folder "Selamatkan" yang berada pada drive E:. Bukalah folder tersebut terlebih dahulu, kemudian klik pada toolbar **History**.



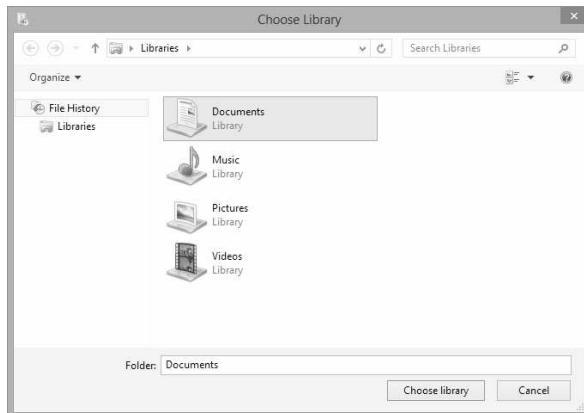
Gambar 9.6 Klik History

Oleh karena kita belum pernah mem-backup folder tersebut maka dari tampilan berikutnya yang muncul disebutkan bahwa file tersebut belum di-backup. Klik pada link **Add it to a library**.



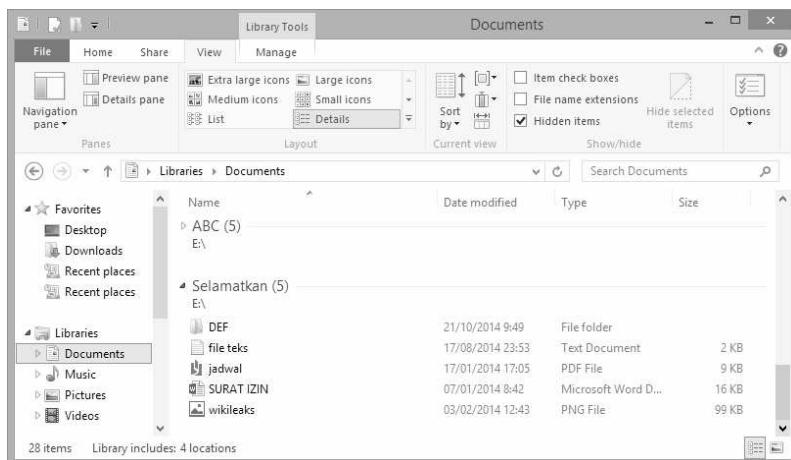
Gambar 9.7 Add it to library

Selanjutnya dalam kotak dialog *Choose Library*, pilih saah satu *library* yang digunakan. Sebagai contoh saya akan memilih *Documents* dan klik tombol **Choose library**.



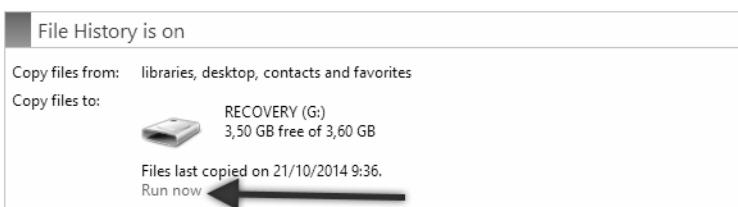
Gambar 9.8 Kotak dialog Choose Library

Sekarang folder “Selamatkan” telah berada dalam *library Documents*.



Gambar 9.9 *Backup folder Selamatkan*

Setelah itu, kembali pada tampilan *File History*, sekarang Anda hanya perlu mengklik **Run now**.



Gambar 9.10 *Run now*

Dan tunggu lah proses penyalinan file dilakukan sampai selesai. Setelah langkah di atas selesai, kini Anda bisa melihat dalam flashdisk tepatnya dalam folder FileHistory, kini telah muncul sebuah folder baru, sesuai dengan nama folder yang Anda buat backup.

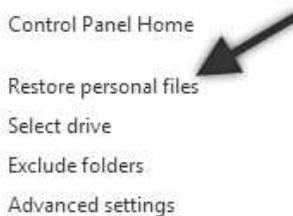
Dari gambar di bawah dalam folder data ada sebuah subfolder bertuliskan E. Hal ini karena folder “Selamatkan” aslinya berasal dari drive E:.

Name	Date modified	Type
ABC	21/10/2014 9:46	File folder
Selamatkan	21/10/2014 9:58	File folder

Gambar 9.11 Folder Selamatkan yang dibackup

9.2 Mengembalikan Data

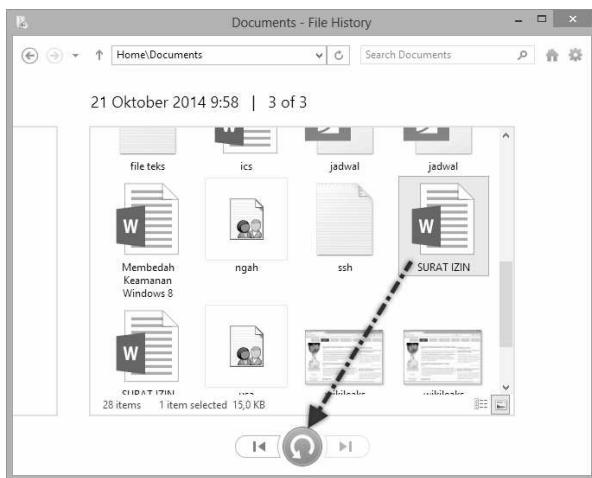
Entah apa yang terjadi, baik sengaja atau tidak tiba-tiba salah satu file dalam folder “Selamatkan” dalam komputer menjadi rusak atau hilang. Sekaranglah saatnya kita membutuhkan bantuan dari *File History* untuk mengembalikan data tersebut. Dari panel sebelah kiri halaman *File History*, klik **Restore personal files**.



Gambar 9.12 Restore personal files

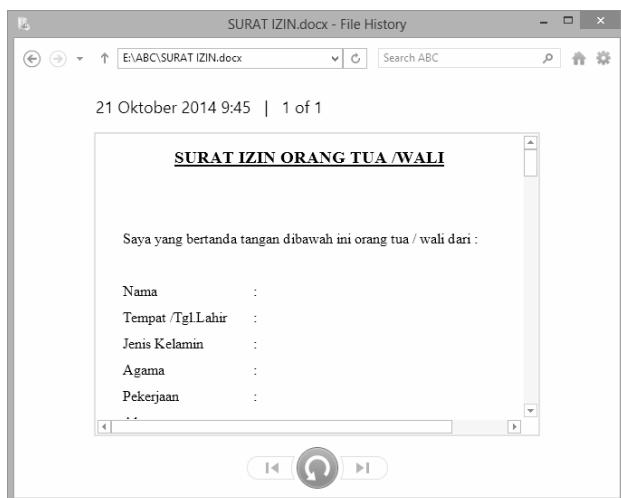
Sejurus kemudian, Anda akan melihat beberapa bentuk folder dan librari yang sama. Yang membedakan adalah tanggal backup. Oleh karena itu, untuk mengembalikan file Anda yang bermasalah, ingatlah tanggal berapa Anda melakukan backup untuk file atau folder tersebut dalam kondisi normal (kalau file Anda error), atau sebelum file tersebut hilang. Selanjutnya, klik pada librari tempat Anda menaruh file backup tersebut. Seperti contoh sebelumnya kita menggunakan librari *Documents*. Klik dua kali pada librari tersebut maka akan tampil nama-nama file yang pernah ada sebelumnya.

Sekarang klik pada nama file yang ingin Anda kembalikan, dan klik tombol **Restore to original location** yang berupa tanda panah melingkar.



Gambar 9.13 Memilih file yang akan di-restore

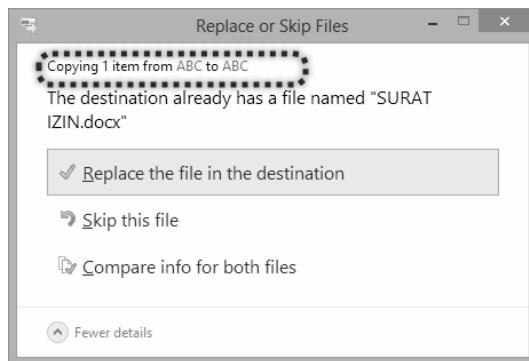
Apabila file yang Anda pilih benar maka file tersebut akan dikembalikan lagi pada foldernya yang semula. Namun, apabila Anda memiliki beberapa file dengan nama yang sama, Anda bisa melakukan double klik untuk mempreview atau melihat isi file tersebut terlebih dahulu.



Gambar 9.14 Preview isi file

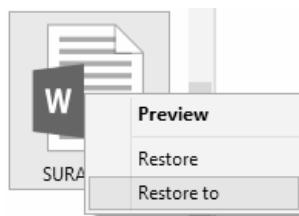
Apabila Anda masih ragu, apakah file tersebut yang akan dikembalikan. Maka sewaktu Anda menekan ikon *Restore to original location* untuk file yang berbeda lokasi maka akan muncul kotak dialog *Replace or Skip Files*.

Jika kita lihat dari gambar di bawah ini, bahwa file tersebut bukanlah file yang berada dalam folder “Selamatkan” melainkan sebuah folder lain yang bernama “ABC”. Sehingga Anda bisa mencari file lainnya yang lebih tepat.



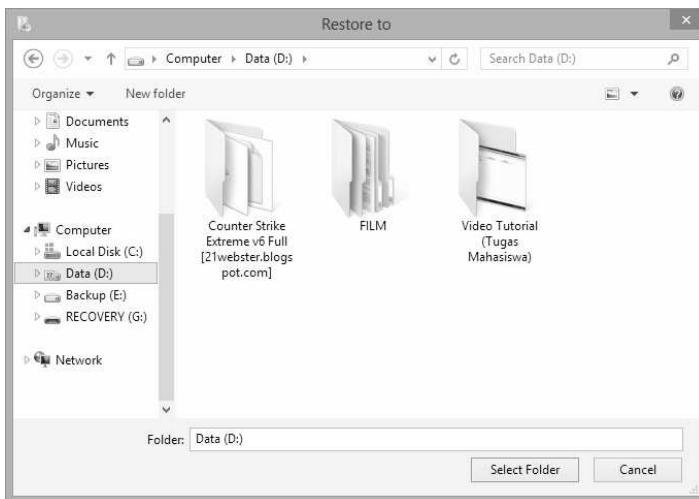
Gambar 9.15 Menyalin file

Kotak dialog di atas juga akan muncul apabila yang terjadi pada file Anda hanyalah rusak atau ada perubahan dalam arti kata bukan hilang. Apabila Anda ragu, akan menindih file yang telah ada, untuk mengembalikan file Anda, maka Anda bisa menggunakan perintah **Restore to**, dengan cara melakukan klik kanan pada file yang akan dikembalikan.



Gambar 9.16 Opsi Restore to

Selanjutnya, dalam kotak dialog *Restore to*, carilah di folder mana Anda ingin menaruh file tersebut. Setelah selesai, klik tombol **Select Folder**.



Gambar 9.17 Kotak dialog *Restore to*

Dengan cara ini maka file lama tidak akan ditindih, dan Anda bisa membuka kedua file tersebut.

9.3 Mempercepat Proses Backup

Jika Anda perhatikan dari contoh di atas, *File History* akan menyalin file yang terdapat dalam folder *Libraries*, *desktop*, *contact*, dan *favorites*. Supaya proses backup bisa berjalan lebih cepat maka Anda bisa melarang *File History* untuk tidak membackup dari folder tertentu. Sebagai contoh kita bisa menghapus pilihan untuk mem-backup folder *Music*, *Pictures*, dan *Videos* yang merupakan subfolder *Libraries*.

Untuk melakukan hal ini, pada panel sebelah kiri *File History*, klik pada menu **Exclude folders**. Pada pemakaian pertama kali, kita belum melarang backup folder apapun, klik tombol **Add** untuk memilih folder yang akan di *exclude* (dikeluarkan).

Exclude from File History

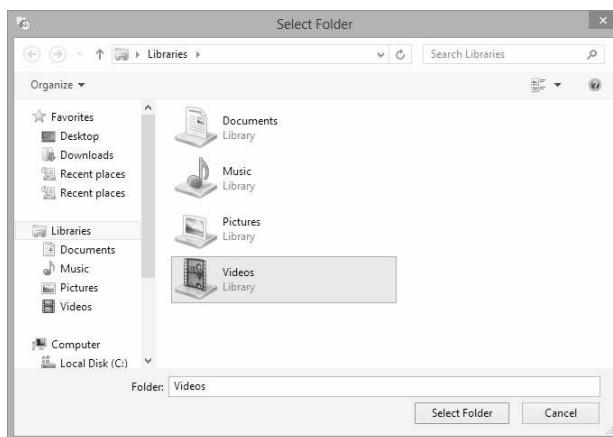
If you don't want to save copies of specific folders or libraries, add them here.

Excluded folders and libraries:



Gambar 9.18 Klik Add

Dari kotak dialog *Select Folder*, carilah folder yang akan di-exclude. Misalnya, saya akan mlarang backup folder *Videos*, klik pada folder tersebut lalu klik tombol **Select Folder**.



Gambar 9.19 Kotak dialog Select Folder

Kini folder *Videos* yang Anda pilih akan berada dalam tempat yang disediakan.

Exclude from File History

If you don't want to save copies of specific folders or libraries, add them here.

Excluded folders and libraries:



Gambar 9.20 Folder yang di-exclude

Lakukan langkah yang sama jika Anda ingin melarang backup untuk folder lainnya. Terakhir jangan lupa klik tombol **Save changes** yang berada pada bagian paling bawah jendela kerja.

9.4 Tips

Demi keamanan dan kenyamanan data Anda, proses backup sangat penting dilakukan. Jika Anda membackup file dalam sebuah flashdisk maka jangan sampai flashdisk tersebut ikut hilang karena data-data Anda akan hilang bersamanya.

10 RECOVERY

Setelah dalam bab sebelumnya, Anda mempelajari bagaimana mengembalikan data yang hilang atau rusak. Sekarang kita akan membahas bagaimana menangani sistem Windows itu sendiri yang bermasalah. Apalagi permasalahan yang terjadi sering kali setelah Anda menginstall software tertentu atau sebuah driver. Komputer Anda bukannya menjadi lebih baik, tapi malah semakin error atau berlaku aneh. Salah satu solusi untuk mengatasi masalah tersebut adalah memanfaatkan fasilitas *recovery* yang telah disediakan oleh Windows 8.

Recovery adalah salah satu fitur yang digunakan untuk mengembalikan setting Windows pada kondisi sebelumnya. Dengan adanya fitur ini maka kita dapat membatalkan perubahan terhadap sistem komputer tanpa harus kehilangan file pribadi milik kita.

Menu *Recovery* ini terdapat dalam Control Panel.

Advanced recovery tools



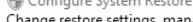
Create a recovery drive

Create a recovery drive to refresh or reset your PC, or to troubleshoot problems, even when it can't start.



Open System Restore

Undo recent system changes, but leave files such as documents, pictures, and music unchanged.



Configure System Restore

Change restore settings, manage disk space, and create or delete restore points.

If you're experiencing problems with your PC, you can refresh it in PC settings.

Gambar 10.1 Advanced recovery tools

Fasilitas Recovery menyediakan beberapa fitur, yaitu:

- *Create a recovery drive* berfungsi untuk menangani masalah terhadap komputer dengan cara membuat sebuah *drive recovery* yang berguna untuk me-refresh atau me-reset komputer.
- *Open system restore* berfungsi untuk membatalkan atau kembali ke sistem yang lama namun file pribadi Anda akan tetap aman.
- *Configure System Resotre* berfungsi untuk mengatur *resotre* dan mengelola *space* harddisk membuat atau menghapus *restore point*.

Yang disebut dengan *restore point* adalah titik atau kondisi di mana komputer Anda dalam keadaan normal.

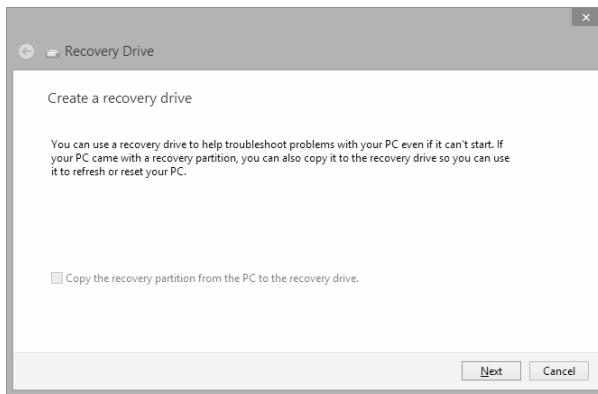
Jika Anda perhatikan gambar di atas sebelumnya, pada bagian kiri menu terdapat tanda ikon berwarna kuning. Hal ini menunjukkan setiap kali kita akan menjalankan fitur tersebut maka akan tampil terlebih dahulu kotak dialog *User Account Control* dan Anda harus memilih Yes untuk bisa menggunakannya.



Gambar 10.2 *User Account Control*

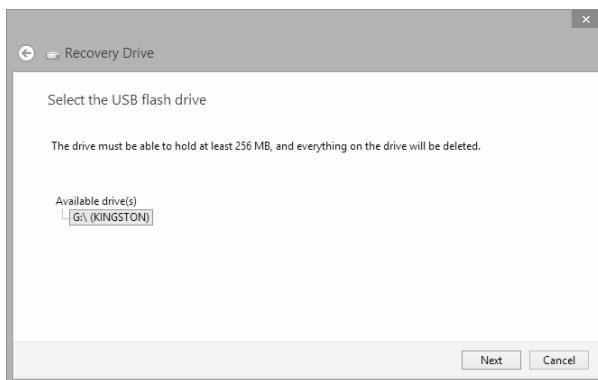
10.1 Membuat Recovery Drive

Pertama-tama kita akan membuat *Recovery Drive*. Mulailah dengan mengklik pada link **Create a recovery drive** maka akan tampil kotak dialog pertama yang menjelaskan fungsi dari *Recovery Drive* tersebut. Dari kotak dialog tersebut, klik tombol **Next** untuk melanjutkan.



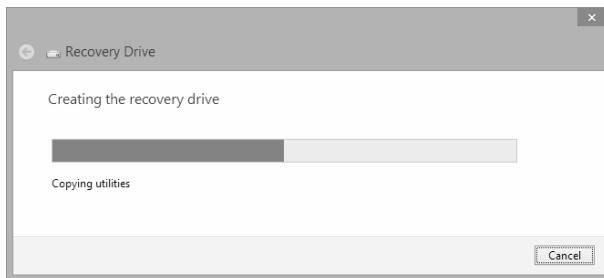
Gambar 10.3 Siap membuat recovery drive

Tungguhlah proses dilakukan, dan pastikan drive USB flashdisk Anda terpasang dan bisa dideteksi seperti gambar di bawah ini. Lanjutkan dengan mengklik tombol **Next**.



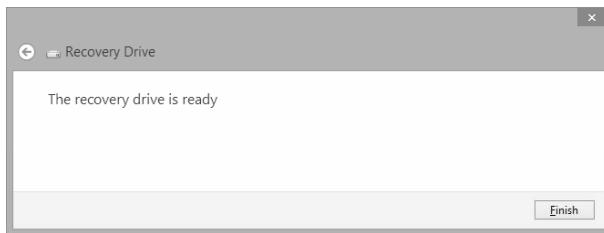
Gambar 10.4 Memilih flashdisk

Sebelum dimulainya proses pembuatan *Recovery Drive* Anda akan diingatkan terlebih dahulu bahwa semua file dalam flashdisk tersebut akan dihapus. Jadi, pastikan Anda telah menyalinnya terlebih dahulu. Jika Anda sudah yakin, klik tombol **Create**. Tungguhlah proses pembuatan *Recovery Drive* selesai dilakukan. Pada awal proses flashdisk Anda akan diformat terlebih dahulu supaya bersih.



Gambar 10.5 Proses pembuatan recovery drive

Setelah proses selesai, dan apabila semuanya lancar-lancar saja maka akan tampil pesan *The recovery drive is ready*. Terakhir, klik tombol **Finish**.



Gambar 10.6 Pembuatan recovery drive selesai

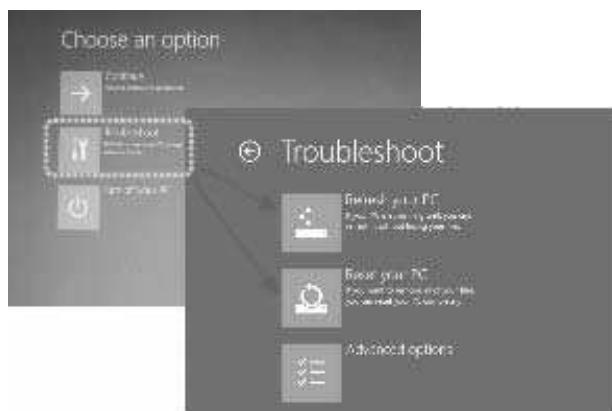
10.2 Refresh Windows

Setelah kita memiliki *Recovery Drive*, yang menjadi pertanyaan adalah untuk apa dan kapan kita perlu menggunakan flashdisk tersebut? Untuk menggunakannya, tentu saja apabila Anda merasa bahwa komputer Anda error, bertindak aneh dan sejenisnya.

Sebelum menggunakan *Recovery Drive* ini sangat disarankan bagi Anda untuk mem-backup data yang ada dalam komputer.

Cara menggunakannya, pertama kali Anda harus mengubah setting BIOS komputer Anda supaya bisa booting melalui flashdisk. Cara setting BIOS untuk setiap jenis komputer berada pada lokasi yang berbeda-beda, jadi tidak dapat saya jelaskan pada bagian ini.

Saya asumsikan komputer Anda bisa *booting* menggunakan flashdisk. Setelah komputer Anda booting menggunakan flashdisk, maka pada tampilan pertama pada bagian *Choose an option*, klik **Troubleshoot**. Selanjutnya pada pilihan *Troubleshoot* Anda bisa memilih *Refresh your PC* atau *Reset your PC*.



Gambar 10.7 Opsi Troubleshoot

Untuk pengetahuan Anda, berikut adalah perbedaan Anda *Refresh your PC* dan *Reset your PC*.

- *Refresh your PC*. Pilihan ini berguna untuk menginstall ulang Windows 8 tanpa mempengaruhi file pribadi dalam komputer kita. Kita bisa menggunakan fitur ini untuk menangani masalah pada Windows, termasuk juga kalau Windows tidak bisa restart. Perlu Anda ketahui juga, walaupun disebutkan proses ini tidak mempengaruhi file pribadi Anda, tapi sangat disarankan Anda tetap membuat backup dari semua file yang ada dalam komputer Anda. Berdasarkan pengalaman pribadi saya, tindakan *refresh* terkadang juga akan menghapus file dalam komputer. Jadi, lebih baik sedia payung sebelum hujan, bikin backup sebelum hilang.
- *Reset your PC*. Pada pilihan yang kedua ini semua file pribadi dan setting Windows akan dihapus dan dikembalikan ke kondisi awal.

Setelah Anda memilih salah satu dari fungsi di atas maka akan tampil informasi, mengenai pilihan Anda tersebut, mengenai tindakan apa saja yang akan dilakukan. Setelah itu, klik **Next**.



Gambar 10.8 Tampilan pilihan Reset dan Refresh

Selanjutnya, Anda diminta untuk memilih sistem operasi yang akan di-refresh atau di-reset. Hal ini terutama sekali bagi Anda yang menginstall lebih dari satu buah sistem operasi. Pada gambar di bawah ini, saya hanya menggunakan satu sistem operasi saja. Jadi kita tinggal klik pada nama Windows 8.



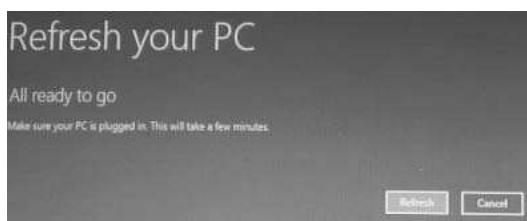
Gambar 10.9 Memilih Refresh your PC

Apabila Anda pernah mencabut flashdisk atau komputer tidak bisa membaca dengan baik flashdisk maka akan tampil pesan untuk memasukkan flashdisk tersebut. Jika ini terjadi, cobalah melepas dan memasukkan kembali flashdisk Anda.



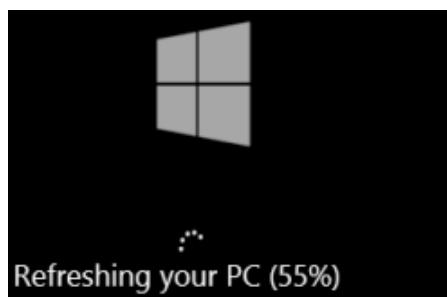
Gambar 10.10 Proses Refresh atau Reset siap dijalankan

Setelah Anda memasang flashdisk, proses selanjutnya segera ditampilkan. Sebagai contoh, berikutnya saya akan mengambil proses *Refresh* saja. Sekarang, Anda telah siap untuk melakukan *refresh*, klik tombol **Refresh** untuk memulai proses.



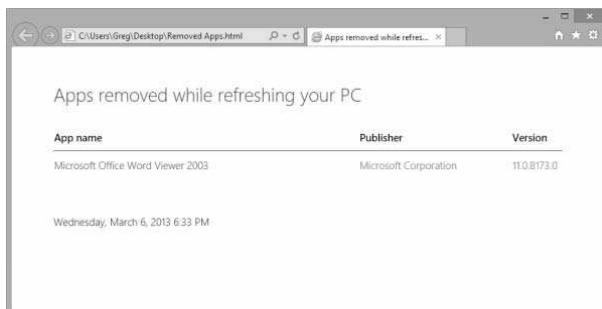
Gambar 10.11 Proses refresh siap dilakukan

Kini tunggu lah proses *refresh* dilakukan sampai selesai.



Gambar 10.12 Proses refresh

Setelah semua proses selesai dijalankan dan kembali pada desktop Windows. Jika di desktop terdapat sebuah file yang bernama *Remove Apps.html*, file tersebut berisikan informasi mengenai program yang telah dihapus dan tidak dilakukan install ulang lagi.



Gambar 10.13 Informasi program yang dihapus

Untuk dapat menggunakan program yang telah dihapus tersebut maka Anda harus menginstallnya kembali.

Demikianlah contoh penerapan *Recovery Drive* untuk melakukan *refresh Windows*. Pada dasarnya untuk me-reset Windows langkah yang ditempuh tidak jauh beda, jadinya saya lewatkan saja.

10.3 Melihat System Restore

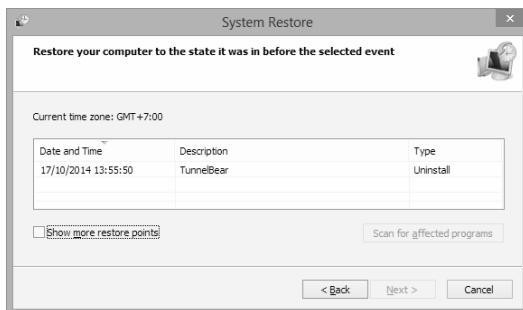
Apabila sebelumnya, kita telah membahas pembuatan dan penggunaan *Recovery Drive*, yang pada dasarnya ditujukan untuk kerusakan pada skala menengah ke atas. *System Restore* digunakan untuk mengembalikan kondisi Windows pada waktu tertentu.

Untuk melihat *System Restore* dalam komputer kita, klik pada **Open System Restore** dalam halaman *Recovery*. Pada tampilan pertama *System Restore* dijelaskan bahwa *System Restore* bisa digunakan untuk mengatasi masalah komputer yang berjalan lambat dan juga *stop responding*. Dikatakan juga bahwa *System restore* tidak akan menghapus file pribadi milik Anda, namun file-file program dan driver akan terhapus sesuai dengan waktu konfigurasi yang Anda pilih. Dari halaman tersebut, lanjutkan dengan mengklik tombol **Next**.



Gambar 10.14 Halaman pertama System Restore

Pada gambar di bawah ini terlihat bahwa, terdapat satu kondisi *system restore*. Di mana saya menghapus atau meng-uninstall program Tunnelbear pada tanggal 17-10-2014. Jadi, nantinya pada tanggal itulah sistem komputer saya akan dikembalikan.



Gambar 10.15 Tanggal restore point

Untuk mengetahui apakah juga terdapat tanggal sistem restore lainnya, berikan tanda centang pada bagian **Show more restore points**. Terlihat dari gambar di bawah ini, muncullah dua *system restore* lagi. Pilih pada tanggal berapa komputer Anda akan di-restore atau dikembalikan pada kondisi sistem sesuai tanggal yang dipilih.

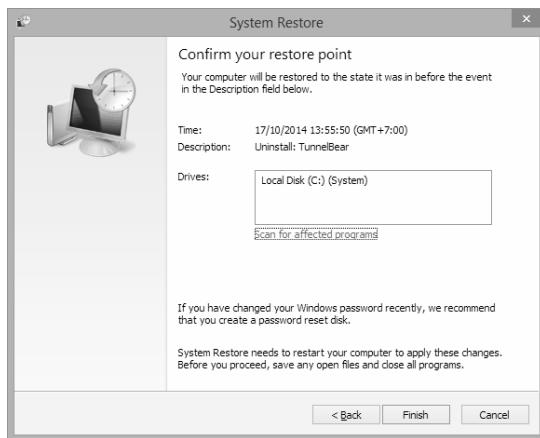
Date and Time	Description	Type
17/10/2014 13:55:50	TunnelBear	Uninstall
13/10/2014 20:46:21	Automatic Restore Point	System
03/10/2014 13:54:33	Automatic Restore Point	System

Show more restore points Scan for affected programs

Gambar 10.16 Restore point yang disembunyikan

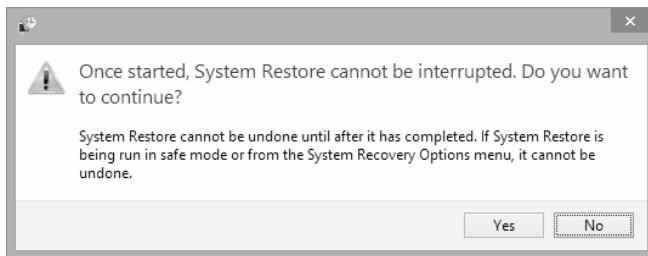
Setelah Anda memilih salah satu *system restore* yang tersedia, klik **Next**.

Berikutnya, akan tampil kotak dialog konfirmasi untuk memastikan bahwa Anda benar-benar akan melakukan *restore*. Jika Anda setuju, klik tombol **Finish** maka proses *restore* segera dilakukan.



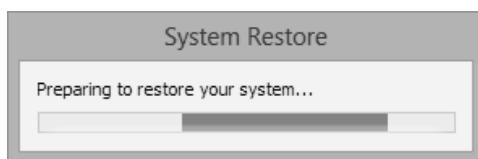
Gambar 10.17 Konfirmasi restore point

Sekali lagi Anda akan ditanyai oleh komputer untuk memastikan Anda benar-benar yakin akan menggunakan *System Restore*. Hal ini ditandai dengan pertanyaan “Sekali dijalankan, *System Restore* tidak dapat diinterupsi. Apakah Anda ingin melanjutkan?”



Gambar 10.18 Peringatan System Restore

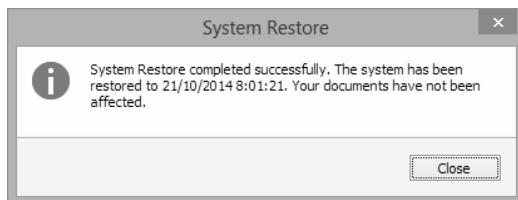
Maksudnya, jika Anda yakin untuk lanjut, prosesnya tidak bisa dihentikan di tengah jalan. Apalagi *System Restore* yang diaktifkan dari kondisi *safe mode* maka tidak bisa dikembalikan lagi ke kondisi sekarang. Apabila hati Anda sudah mantap, klik tombol **Yes**. Selanjutnya komputer segera mempersiapkan dirinya untuk *me-restore* sistem komputer.



Gambar 10.19 Pesiapan proses restore

Sewaktu proses *restore* dilakukan, komputer akan melakukan restart. Jadi, sebaiknya Anda menyimpan semua pekerjaan Anda terlebih dahulu. Sekarang, tunggu prosesnya sampai selesai.

Apabila proses *restore* telah dilakukan maka sewaktu komputer aktif kembali akan tampil pesan bahwa *System Restore* telah sukses dijalankan. Terakhir klik tombol **Close**.

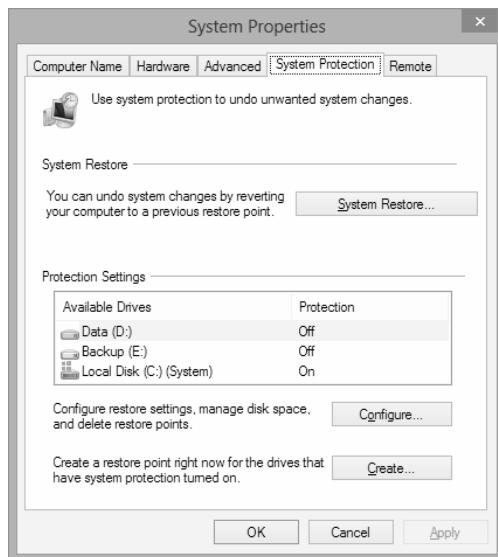


Gambar 10.20 System Restore selesai dilakukan

10.4 Konfigurasi System Restore

Setelah sebelumnya Anda bisa me-*restore* komputer pada kondisi sesuai dengan tanggal yang Anda pilih. Sekarang waktunya untuk melakukan konfigurasi terhadap *System Restore*. Hal ini bisa Anda lakukan dengan mengklik pilihan **Configure System Restore** pada halaman *Recovery*.

Berikut tampilan setelah Anda mengklik *Configure System Restore*.

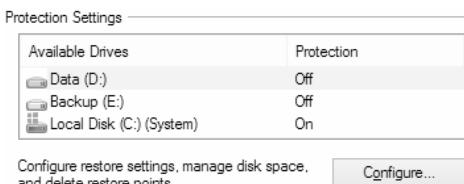


Gambar 10.21 System Protection

Dari gambar di atas, tombol **System Restore** berfungsi untuk membuka halaman kerja *System Restore* seperti yang telah kita lakukan sebelum ini. Sekarang yang menjadi perhatian kita adalah bagian *Protection Settings*.

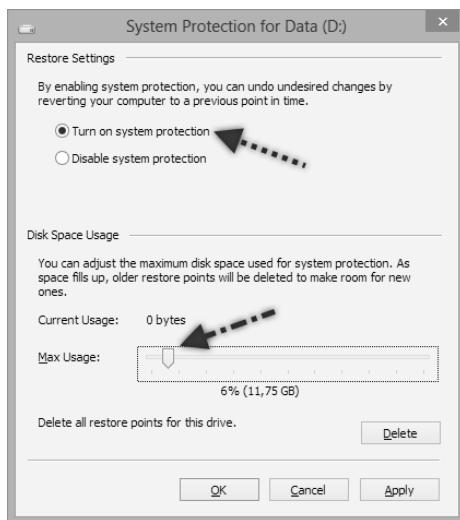
Secara default drive yang diaktifkan atau dilindungi oleh *System Restore* adalah drive C:. Hal ini ditandai dengan statusnya yang bertuliskan *On*. Pengaktifan *System Restore* pada bagian ini dikarenakan file sistem Windows ada pada drive tersebut.

Jika Anda ingin drive lainnya, ikut dilindungi dengan *System Restore* juga maka klik pada salah satu drive dan klik tombol **Configure**.



Gambar 10.22 Memilih drive

Dari kotak dialog *System Protection* yang muncul, berikan pilihan pada bagian **Turn on system protection**. Di bawahnya, geserlah *slider* berapa persen ruang harddisk yang akan digunakan untuk menyimpan file *System Restore*. Sebagai contoh, di bawah ini saya mengalokasikan 6% ruang harddisk sebagai penyimpanan *restore point*. Terakhir klik tombol **OK**.



Gambar 10.23 Mengaktifkan sistem proteksi

Kini perhatikanlah pada bagian drive D:, yang status proteksinya telah berubah menjadi *On*. Dalam kotak dialog ini juga terdapat sebuah tombol *Delete* yang berfungsi untuk menghapus semua file *restore point* yang pernah disimpan.



Gambar 10.24 Sistem proteksi drive D: aktif

10.5 Membuat Restore Point

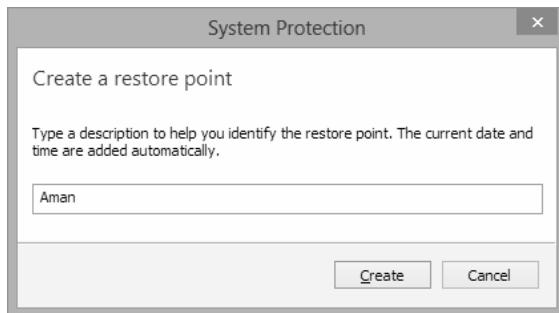
Sekarang kita akan membuat sebuah *restore point*, tujuannya adalah untuk mencegah terjadinya hal-hal yang tidak diinginkan pada komputer. Misalnya begini, tatkala Anda hendak menginstall sebuah program, driver, atau mungkin Anda sedang belajar bikin virus. Sebelum semua tindakan tersebut Anda lakukan ada baiknya Anda membuat sebuah *restore point* terlebih dahulu. Tujuannya adalah supaya ketika Anda selesai menginstall program atau driver tersebut, komputer Anda menjadi aneh, alias error atau rusak. Maka Anda bisa mengembalikan kondisi komputer Anda pada keadaan saat *restore point* dibuat (tepat sebelum Anda menginstall program atau driver). Tentu saja, pastikan sewaktu membuat *restore point* komputer Anda sedang dalam kondisi normal.

Baiklah, mari kita mulai membuat *restore point*. Pertama-tama bukalah kotak dialog *System Properties* seperti penjelasan di atas. Klik pada tombol yang paling bawah dengan tulisan **Create**.



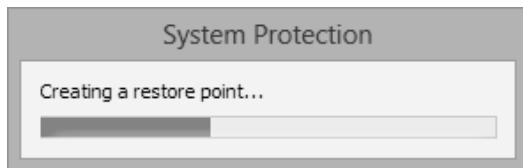
Gambar 10.25 Klik Create

Berikutnya muncul kotak dialog yang meminta Anda untuk memasukkan nama *restore point*. Sebagai contoh di bawah ini saya menggunakan nama "Aman". Lanjutkan dengan mengklik tombol **Create**.



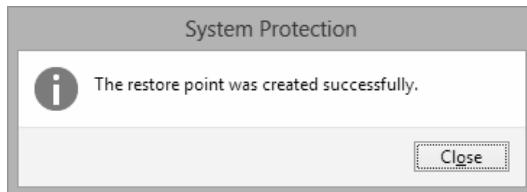
Gambar 10.26 Membuat restore point

Tungguah proses pembuatan *restore point* dilakukan sampai selesai.



Gambar 10.27 Proses pembuatan restore point

Setelah selesai maka muncul pesan *The restore point was created successfully*. Klik saja tombol **Close**.



Gambar 10.28 Pembuatan restore point selesai

Untuk memastikan bahwa *restore point* telah berhasil dibuat, klik tombol **System Restore**. Kini sebuah *restore point* baru yang bernama "Aman" telah berada dalam halaman *System Restore*.

Date and Time	Description	Type
21/10/2014 8:01:21	Aman	Manual
17/10/2014 13:55:50	TunnelBear	Uninstall

Gambar 10.29 Daftar restore point

Selanjutnya barulah Anda bebas mengotak-atik komputer Anda, dan apabila terjadi hal-hal yang tidak diinginkan maka Anda bisa me-restore ke kondisi “Aman” tersebut. Caranya? Tentu saja sudah kita bahas dalam subbab sebelumnya.

10.6 Tips

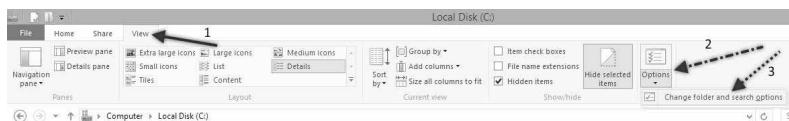
Seperti yang pernah dijelaskan sebelumnya bahwa *System Restore* menyimpan informasi perubahan dalam bentuk file karena memakan ruang harddisk. Jika Anda ingin tahu, di mana lokasi penyimpanan filenya, adalah di: C:\System Volume Information.

Folder tersebut akan terlihat apabila Anda mengaktifkan fungsi untuk menampilkan file *hidden* dan file system. Sebagai contoh, secara normal, folder yang terlihat pada drive C: dalam komputer saya adalah seperti gambar di bawah ini.

Computer > Local Disk (C:)			
	Name	Date modified	Type
Favorites			
Desktop	Intel	28/10/2013 6:45	File folder
Downloads	MSOCache	27/10/2013 18:31	File folder
Recent places	PerfLogs	26/07/2012 14:33	File folder
Recent places	Program Files	18/10/2014 5:36	File folder
Libraries	Program Files (x86)	18/10/2014 5:13	File folder
Documents	ProgramData	18/10/2014 5:13	File folder
Music	Users	19/10/2014 17:58	File folder
	Windows	21/10/2014 8:12	File folder

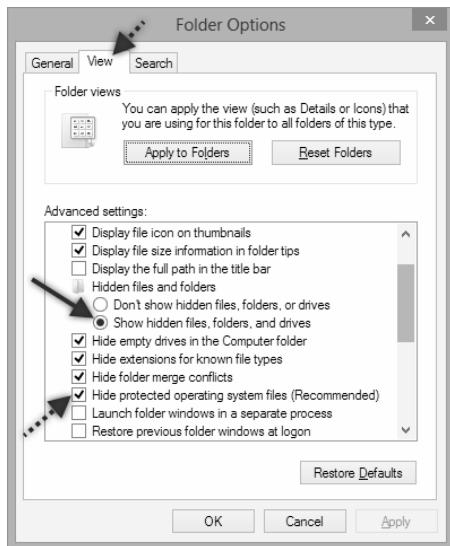
Gambar 10.30 Folder pada C:

Dari gambar di atas, tidak terlihat keberadaan folder *System Volume Information*. Untuk menampilkannya dalam File Explorer klik pada menu **View**. Setelah tampilan berubah, perhatikan pada bagian paling kanan, klik toolbar *Options* dan klik menu di bawahnya yang muncul **Change folder and search options**.



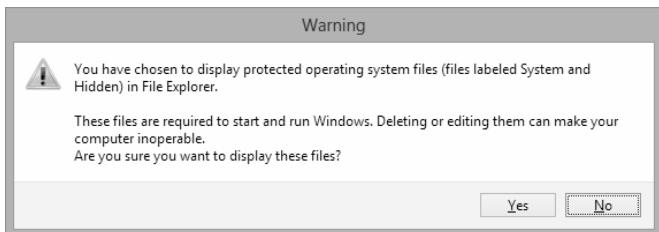
Gambar 10.31 Memilih Change folder and search options

Dalam kotak dialog *Folder Options*, klik tab **View** dan di bawahnya, berikan pilihan pada bagian **Show hidden files, folders, and drives**.



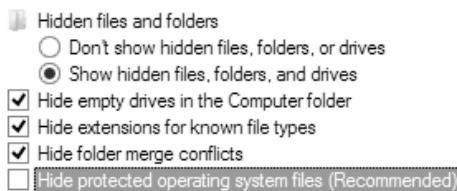
Gambar 10.32 Kotak dialog Folder Options

Masih dalam lokasi yang sama, kali ini perhatikan pada bagian **Hide protected operating system files (Recommended)**. Hilangkan tanda centang pada bagian tersebut. Maka akan muncul pesan peringatan, klik saja **Yes**.



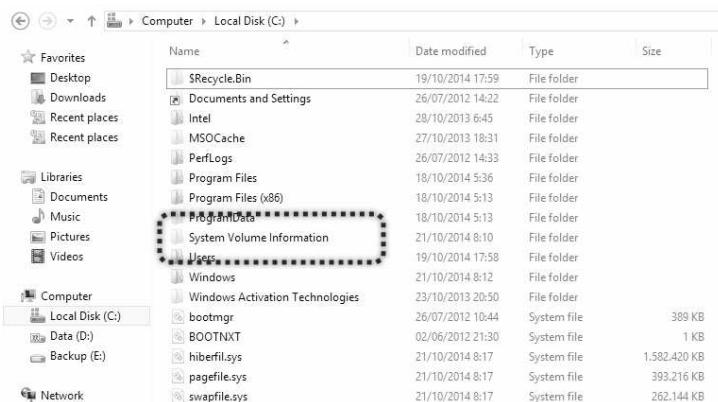
Gambar 10.33 Pesan peringatan

Setelah kembali pada kotak dialog *Folder Options*, barulah tanda centang tersebut hilang.



Gambar 10.34 Hide protected operating system files

Terakhir klik tombol **OK**. Kini folder *System Volume Information* telah tampil. Malangnya, kita tidak diizinkan untuk membuka folder tersebut. Maaf sekali, buku ini tidak menjelaskan cara membobol keamanan, jadi biarkan saja apa adanya. Namun, jika Anda tertarik untuk mengetahui sistem pengamanan seperti ini, ada satu buku bagus yang bisa saya ajukan sebagai referensi yaitu buku yang berjudul “Anti Privacy: Melacak, Membajak & Membobol Data Rahasia”.



	Name	Date modified	Type	Size
★ Favorites	\$Recycle.Bin	19/10/2014 17:59	File folder	
Desktop	Documents and Settings	26/07/2012 14:22	File folder	
Downloads	Intel	28/10/2013 6:45	File folder	
Recent places	MSOCache	27/10/2013 18:31	File folder	
Recent places	PerfLogs	26/07/2012 14:33	File folder	
Libraries	Program Files	18/10/2014 5:36	File folder	
Documents	Program Files (x86)	18/10/2014 5:13	File folder	
Music	ProgramData	18/10/2014 5:13	File folder	
Pictures	System Volume Information	21/10/2014 8:10	File folder	
Videos	Users	19/10/2014 17:58	File folder	
Computer	Windows	21/10/2014 8:12	File folder	
Local Disk (C:)	Windows Activation Technologies	23/10/2013 20:50	File folder	
Computer	bootmgr	26/07/2012 10:44	System file	389 KB
Data (D:)	BOOTNXT	02/06/2012 21:30	System file	1 KB
Backup (E:)	hiberfil.sys	21/10/2014 8:17	System file	1,582,420 KB
Network	pagefile.sys	21/10/2014 8:17	System file	393,216 KB
	swapfile.sys	21/10/2014 8:17	System file	262,144 KB

Gambar 10.35 Folder System Volume Information

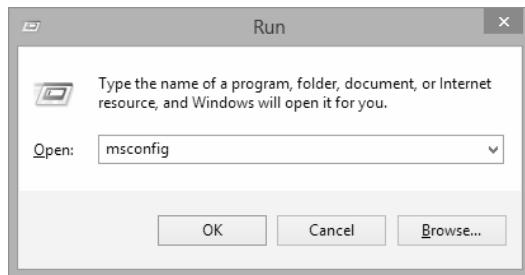
11 SYSTEM CONFIGURATION

Terdapat banyak konfigurasi sistem operasi Windows 8 yang berguna untuk mengendalikan sistem operasi, dapat dilakukan dalam *System Configuration* atau lebih dikenal dengan sebutan *msconfig*. Untuk memanggil *System Configuration* ini, Anda bisa mengetikkan langsung kata "msconfig" pada tampilan Start Windows 8 dan hasilnya akan tampil pada bagian sebelah kiri. Lalu dengan menekan *Enter* halaman *System Configuration* akan terbuka.



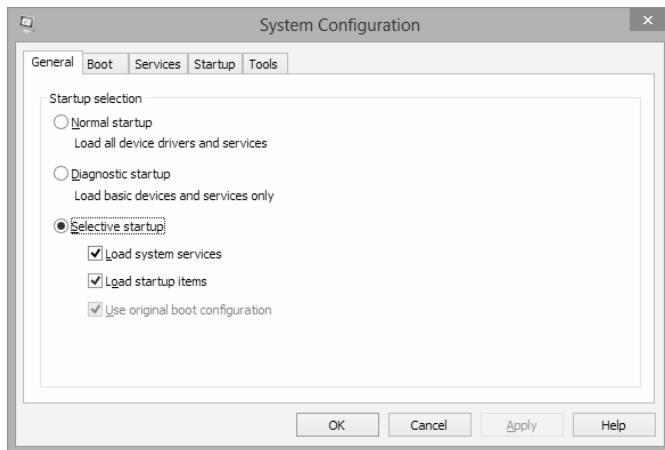
Gambar 11.1 *Msconfig*

Cara lainnya yang umum digunakan adalah dengan menekan kombinasi tombol keyboard, yaitu tombol Windows dan tombol huruf R (**Win + R**) maka akan muncul kotak dialog *Run*. Dalam kotak dialog tersebut ketiklah **msconfig** kemudian tekan *Enter* atau klik tombol **OK** maka *System Configuration* akan tampil.



Gambar 11.2 Kotak dialog Run

Dalam bab ini kita akan mencoba mengotak-atik *System Configuration* tersebut. Berikut tampilan dari *System Configuration*.



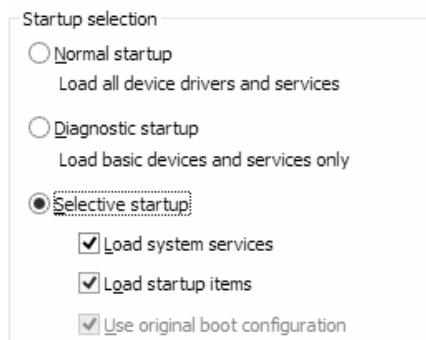
Gambar 11.3 System Configuration

Di dalamnya, terdapat beberapa tab, yaitu *General*, *Boot*, *Services*, *Startup*, dan *Tools*. Untuk mempermudah penjelasan maka kita akan membahas isi dan konfigurasi dari masing-masing tab tersebut.

11.1 General

Pada tab *General* terdapat informasi untuk memilih model *Startup* yang akan dilakukan oleh Windows. Pilihan tersebut adalah:

- *Normal startup*: digunakan untuk menjalankan semua driver dan service Windows sewaktu *booting*.
- *Diagnostic startup*: digunakan apabila kita ingin Windows hanya menjalankan *device* dan *service* yang dasar dan yang standar saja.
- *Selective startup*: pada bagian ini kita dapat memilih apa saja yang akan dijalankan oleh Windows sewaktu pertama kali diaktifkan (*booting*). Secara default pilihan yang aktif adalah *Selective startup* dengan pilihan *Load system services*, *Load startup items*, dan *Use original boot configuration*. Kita dapat memilih salah satu atau sekaligus semuanya.



Gambar 11.4 Startup selection

Dalam kondisi ini, pemilihan *Selective startup* adalah cara yang aman dari pada kita menjalankan semua service. Sebab, bisa saja ada service yang berbahaya bukan milik Windows. Sedangkan *selective startup* bisa berubah sewaktu kita melakukan konfigurasi pada tab lain nantinya. Pada bagian ini belum ada setting yang menarik untuk kita modifikasi, karena berhubungan dengan tab lain.

11.2 Startup

Sekarang kita langsung saja menuju pada tab *Startup*. Sewaktu membuka tab tersebut isinya hanyalah pesan bahwa untuk mengelola startup dilakukan melalui *Task Manager*. Klik saja pada link **Open Task Manager**.

To manage startup items, use the Startup section of Task Manager.

[Open Task Manager](#)

Gambar 11.5 Isi tab Startup

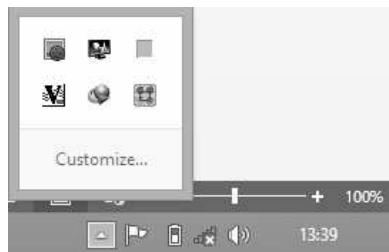
Dari halaman *Task Manager* yang terbuka, ditampilkan daftar program yang aktif sewaktu Windows pertama kali dijalankan (*booting*).

The screenshot shows the Windows Task Manager window with the 'Startup' tab selected. The table lists various startup items with columns for Name, Publisher, Status, and Startup impact. A note at the top right indicates the last BIOS time was 3.6 seconds. At the bottom, there are buttons for 'Fewer details' and 'Disable'.

Name	Publisher	Status	Startup impact
hkcmd Module	Intel Corporation	Enabled	Medium
igfxTray Module	Intel Corporation	Enabled	Medium
Internet Download Manager...	Tonec Inc.	Enabled	High
NokiaInternetModem_AppS...		Enabled	High
persistence Module	Intel Corporation	Enabled	Medium
SoftEther VPN	SoftEther VPN Project at...	Enabled	Medium
SoftEther VPN	SoftEther VPN Project at...	Enabled	High
TightVNC Server	GlavSoft LLC.	Enabled	Low
Yahoo! Messenger	Yahoo! Inc.	Disabled	None

Gambar 11.6 Task Manager

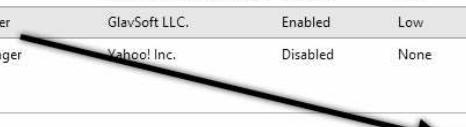
Program-program yang aktif tersebut merupakan program yang berada di systray di sudut kanan bawah atau tersembunyi.



Gambar 11.7 Program yang di-load saat Windows dijalankan

Jika Anda tidak menginginkan program-program tersebut dijalankan oleh Windows sewaktu startup. Maka pada halaman Task Manager, klik pada nama programnya lalu klik tombol **Disable** yang terdapat di bagian bawah.

Name	Publisher	Status	Startup impact
hcmd Module	Intel Corporation	Enabled	Medium
SoftEther VPN	SoftEther VPN Project at...	Enabled	High
TightVNC Server	GlavSoft LLC.	Enabled	Low
Yahoo! Messenger	Yahoo! Inc.	Disabled	None



Gambar 11.8 Memilih Disable

Efeknya, status program yang semula adalah *Enabled* menjadi *Disabled*. Sehingga berikutnya sewaktu Windows dijalankan, program tersebut tidak akan di-load lagi, hasilnya proses booting bisa berlangsung lebih cepat.

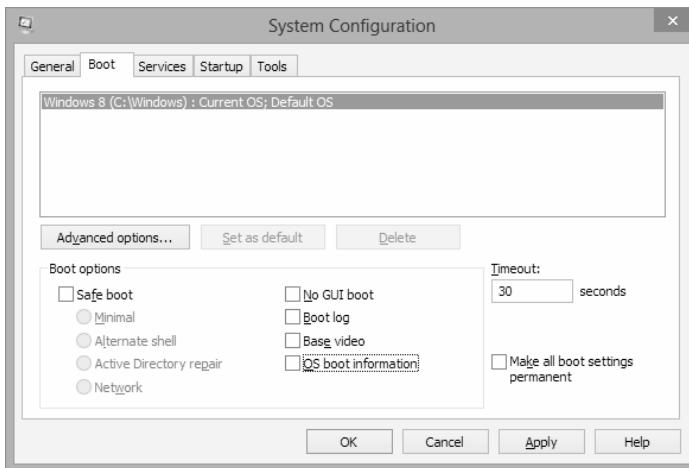
SoftEther VPN	SoftEther VPN Project at...	Enabled	High
TightVNC Server	GlavSoft LLC.	Disabled	Low
Yahoo! Messenger	Yahoo! Inc.	Disabled	None

Gambar 11.9 Status Disabled

Lakukan hal yang sama untuk program-program lainnya. Setelah selesai, tutup saja jendela Task Manager tersebut.

11.3 Boot

Sekarang mari kita tengok tab *Boot*, dalam tab ini berfungsi untuk mengatur berbagai setting Windows sewaktu booting atau sewaktu dijalankan pertama kali. Pada tempat yang tersedia seperti gambar di bawah, tertulis satu buah sistem operasi Windows 8. Apabila dalam komputer Anda menerapkan *dual booting* atau terdapat lebih dari satu sistem operasi dalam satu komputer maka akan tampil juga nama sistem operasi lainnya.



Gambar 11.10 Tab Boot

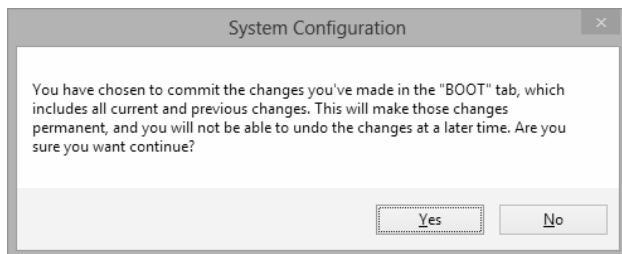
Salah satu setting yang bisa dilakukan seandainya terdapat beberapa sistem operasi maka Anda bisa memilih tombol *Set as default* untuk menerapkan sistem operasi tersebut sebagai sistem operasi utama yang akan dijalankan pertama kali.

Dalam tampilan di atas juga, terlihat bahwa semua file sistem boleh dibilang file inti Windows disimpan dalam folder C:\Windows.

Beberapa setting di bawahnya misalnya, *No GUI boot* berfungsi untuk menghilangkan tampilan Windows sewaktu booting. Namun, hal ini tidak ngefek pada Windows 8 yang hilang hanyalah animasi loading berupa lingkaran. Jika Anda mencoba pada sistem Windows sebelumnya, seharusnya yang tampil adalah file-file yang di-load oleh Windows sewaktu booting. Begitu pula pilihan *OS boot information* juga tidak tampil. Jika diperlukan Anda bisa memilih *Boot log* untuk pembuatan data-data log, dan juga *Base video* untuk menampilkan Windows sesuai standar tampilan mendasar. Kebanyakan efek dari tab ini akan terasa jelas ketika kita menginstall lebih dari satu sistem operasi.

Bagian *Timeout* berfungsi untuk mengatur berapa lama sistem operasi harus menunggu sebelum secara otomatis mengaktifkan Windows (*Time out*). Dan apabila Anda memberikan tanda centang pada bagian *Make all boot settings permanent* maka semua setting yang Anda pilih akan selalu digunakan oleh Windows (dijadikan *default*). Dengan memberikan tanda centang tersebut maka sewaktu Anda klik *Apply* atau

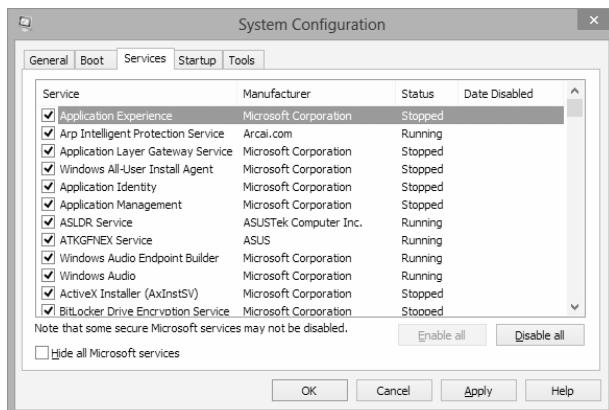
OK akan tampil kotak dialog konfirmasi yang menyatakan apabila Anda memilih pilihan tersebut selanjutnya Anda akan tidak bisa membatalkan perintah yang telah Anda buat tersebut nantinya. Jadi keputusannya terserah pada tangan Anda.



Gambar 11.11 Peringatan sebelum merubah isi tab Boot

11.4 Services

Dalam tab *Services* ini adalah daftar berbagai servis atau layanan yang dijalankan dan umumnya diperlukan oleh Windows. Namun, tidak semua service tersebut adalah milik Microsoft, bisa juga digunakan oleh program lain yang akan mengaktifkan service ini supaya dapat aktif.



Gambar 11.12 Tab Services

Kolom *Status* menunjukkan bahwa program tersebut aktif bekerja (*Running*) atau tidak aktif (*Stopped*).

Jika Anda ingin melihat *services* yang bukan dari Microsoft, berilah tanda centang pada bagian **Hide all Microsoft services**.

Service	Manufacturer	Status	Date Disabled
<input checked="" type="checkbox"/> Arp Intelligent Protection Service	Arcai.com	Running	
<input checked="" type="checkbox"/> ASLDR Service	ASUSTek Computer Inc.	Running	
<input checked="" type="checkbox"/> ATKGFNEX Service	ASUS	Running	
<input checked="" type="checkbox"/> Intel(R) Content Protection HEC...	Intel Corporation	Stopped	
<input checked="" type="checkbox"/> HWDeviceService64.exe	Unknown	Running	
<input checked="" type="checkbox"/> Mozilla Maintenance Service	Mozilla Foundation	Stopped	
<input checked="" type="checkbox"/> MyPublicWiFi Service	Unknown	Running	
<input checked="" type="checkbox"/> Quick Net, OUC	Unknown	Stopped	
<input checked="" type="checkbox"/> Remote Packet Capture Protocol...	Riverbed Technology, Inc.	Stopped	
<input checked="" type="checkbox"/> Service KMSELDI	Unknown	Stopped	
<input checked="" type="checkbox"/> SoftEther VPN Client	SoftEther VPN Project at U...	Running	
<input checked="" type="checkbox"/> TightVNC Server	GlavSoft LLC.	Running	

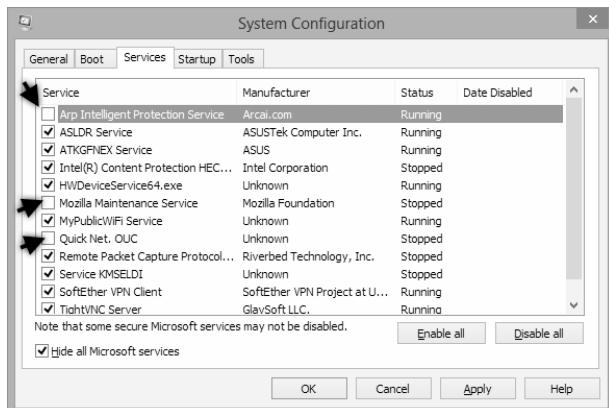
Note that some secure Microsoft services may not be disabled.

Hide all Microsoft services

Gambar 11.13 Daftar servis yang bukan dari Microsoft

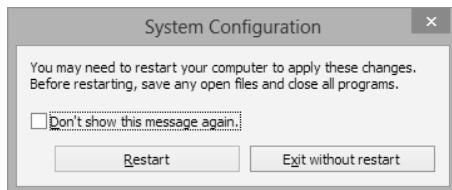
Dapat kita lihat dari gambar di atas, terdapat banyak program lain yang juga memanfaatkan fitur *Services* ini supaya bisa berjalan. Pada dasarnya, jika ada services yang tidak digunakan bisa Anda matikan sebab bisa mempercepat proses booting Windows. Selain itu, jika ada service yang mencurigakan bisa saja digunakan oleh virus lebih baik dinonaktifkan saja.

Cara menonaktifkan sebuah service adalah dengan menghilangkan tanda centang pada bagian depan nama service tersebut. Untuk cara cepat, jika Anda ingin mengaktifkan semua service yang tampil, klik tombol **Disable all**. Namun, berhati-hatilah jika Anda men-disable sebuah service apalagi yang diperlukan oleh program, bisa-bisa program tersebut tidak dapat berjalan lagi.



Gambar 11.14 Men-disable servis

Setelah Anda memilih *service* yang akan dimatikan, klik tombol **OK**. Maka untuk menerapkan perubahan tersebut Anda diminta untuk merestart komputer. Klik tombol **Restart**.



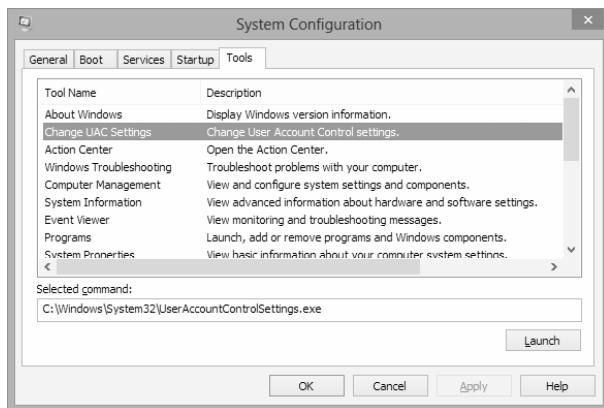
Gambar 11.15 Permintaan restart

Seandainya, Anda masih ingin menggunakan komputer dan belum mau melakukan restart. Anda bisa menunda restart tersebut untuk lain waktu dengan memilih *Exit without restart* maka Anda akan dibawa kembali pada halaman Windows.

11.5 Tools

Penjelasan mengenai tab *Tools* ini tidak akan saya bahas, karena fungsinya hanyalah untuk menjalankan fasilitas-fasilitas yang memang telah ada dalam Windows 8. Misalnya, untuk menjalankan pengaturan *User Accounts Control* seperti yang telah pernah kita bahas dalam bab

awal buku ini. Klik pada bagian **Change UAC Settings** dan klik pula tombol **Launch**.



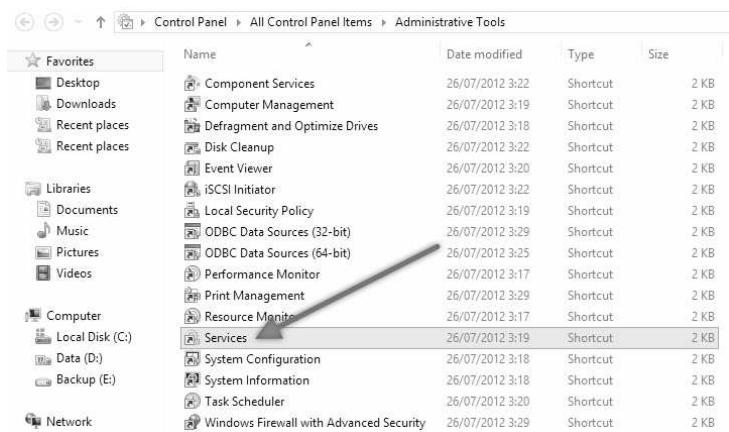
Gambar 11.16 Tab Tools

Selanjutnya akan tampil jendela kerja *User Account Control Settings*. Begitu pula dengan yang *tool* lainnya. Oleh karena itulah tab *Tools* ini tidak saya bahas terlalu detil di sini, boleh dibilang semacam Control Panel sederhana.

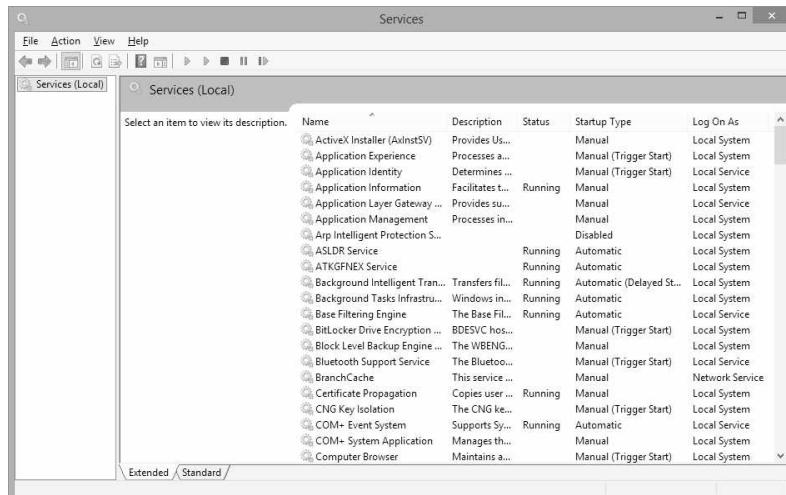
11.6 Tips

Pada subbab *Services* kita telah bisa mengetahui nama-nama servis yang dijalankan oleh Windows. Namun, untuk mengetahui lebih detil serta deskripsi dari servis tersebut maka Anda bisa melakukan langkah berikut:

1. Masuklah ke dalam Control Panel dan jalankan **Administrative Tools**.
2. Dari berbagai pilihan yang tersedia dalam *Administrative Tools*, klik pada **Services**.

**Gambar 11.17 Klik Services**

3. Sekarang jendela kerja Services telah tampil.

**Gambar 11.18 Daftar servis**

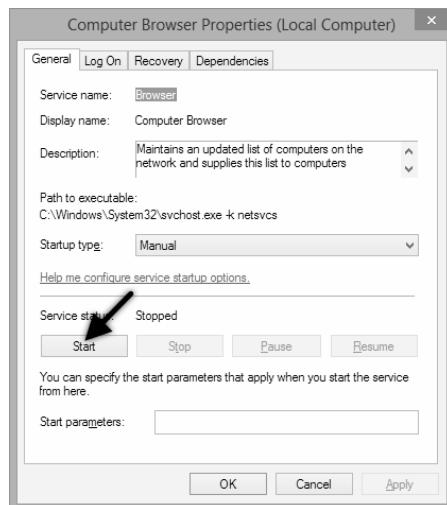
4. Untuk mengetahui penjelasan dan fungsi dari sebuah servis, Anda hanya perlu mengklik satu kali pada nama servis. Maka pada bagian sebelah kiri akan tampil deskripsi dari servis yang Anda pilih tersebut.

Computer Browser	Name	Description	Status	Startup Type	Log On As
Start the service	COM+ Event System	Supports Sy...	Running	Automatic	Local Service
	COM+ System Application	Manages th...	Manual		Local System
Description:	Computer Browser	Maintains a...	Manual (Trigger Start)	Local System	
Maintains an updated list of computers on the network and supplies this list to computers designated as browsers. If this service is stopped, this list will not be updated or maintained. If this service is disabled, any services that explicitly	Credential Manager	Provides se...	Manual		Local System
	Cryptographic Services	Provides thr...	Running	Automatic	Network Service
	DCOM Server Process Laun...	The DCOM...	Running	Automatic	Local System
	Device Association Service	Enables pair...	Running	Automatic (Trigger Sta...	Local System
	Device Install Service	Enables the c...	Running	Manual (Trigger Start)	Local System
	Device Setup Manager	Enables the e...	Running	Manual (Trigger Start)	Local System
	DHCP Client	Registers an	Running	Automatic	Local Service

Gambar 11.19 Penjelasan sebuah servis

Untuk servis dengan status *Running* hal ini berarti servis tersebut sedang berjalan dan digunakan oleh Windows. Apabila pada kolom status kosong berarti servis tersebut tidak diaktifkan. Selanjutnya pada kolom *Startup Type*, terdapat dua jenis, yaitu *Automatic* yang berarti servis tersebut akan dijalankan secara otomatis sewaktu Windows dinyalakan. Sedangkan tipe manual berarti servis tersebut harus diaktifkan secara manual.

Jika diinginkan Anda dapat mematikan atau mengaktifkan sebuah servis. Caranya adalah dengan melakukan double klik pada servis yang Anda pilih, dan dari kotak dialog yang muncul klik tombol **Start** lalu klik **OK**. Atau tombol **Stop** jika ingin mematikan sebuah servis.



Gambar 11.20 Properti servis

Dalam kotak dialog tersebut, juga terdapat pilihan *Startup type* yang berarti kita bisa mengubah servis yang otomatis menjadi manual maupun sebaliknya. Selain itu, perhatikan pada bagian *Path to executable* merupakan penunjuk file yang menggunakan servis tersebut.

12 DATA EXECUTION PREVENTION

Seperti yang kita ketahui ada banyak program-program nakal hingga yang berbahaya dan berniat untuk menyerang sistem Windows. Salah satu cara yang ditempuh oleh program-program tersebut adalah dengan mengeksekusi (*execute*) atau menjalankan kode-kode program pada lokasi memory tertentu. Tentu saja serangan tersebut sangatlah berbahaya bagi kelangsungan hidup Windows kita. Salah satu fitur yang telah disediakan oleh Windows untuk menanggulangi hal-hal yang tidak diinginkan tersebut adalah fitur *Data Execution Prevention* (DEP).

DEP akan bekerja dengan cara memantau program-program dan servis yang berjalan serta memastikan bahwa program tersebut memakai memory dengan aman. Apabila DEP menemukan program yang dianggap akan menyerang sistem Windows maka program tersebut akan ditutup. Dengan demikian kita dapat memanfaatkan DEP untuk meningkatkan keamanan Windows yang kita gunakan.

Pertama-tama kita akan belajar cara menampilkan lokasi kerja DEP. Masuklah ke dalam Control Panel, kemudian klik **System**. Dari halaman *System* yang muncul, perhatikan pada panel sebelah kiri, klik pada menu **Advanced system settings**.

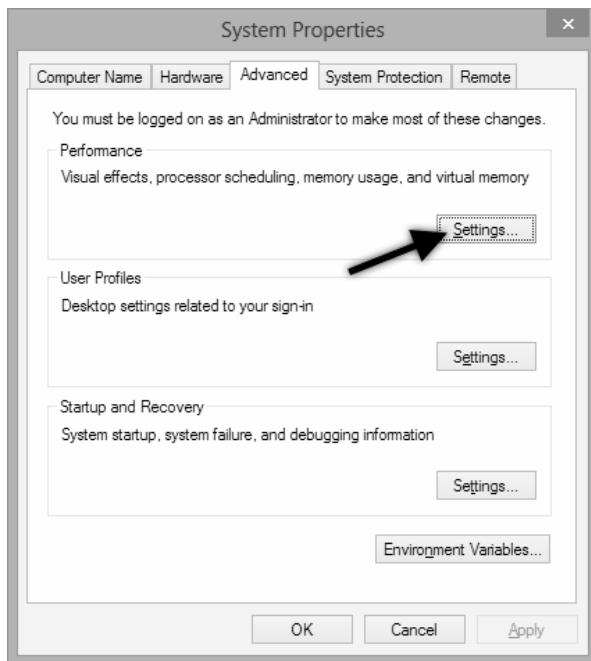
Control Panel Home

-  Device Manager
-  Remote settings
-  System protection
-  Advanced system settings



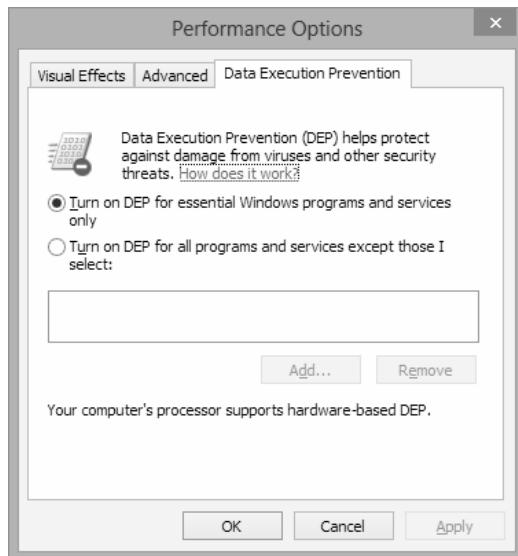
Gambar 12.1 Advanced system settings

Berikutnya akan tampil kotak dialog *System Properties* yang secara otomatis pula akan membuka tab *Advanced*. Dalam kotak dialog tersebut, perhatikan pada bagian *Performance*, klik tombol **Settings**.



Gambar 12.2 Tab Advanced

Maka kan tampil kotak dialog *Performance Options*. Dalam kotak dialog tersebut klik pada tab **Data Execution Prevention**. Pada lokasi inilah kita akan bekerja.



Gambar 12.3 Kotak dialog Performance Options

Perlu Anda ketahui bahwa fitur DEP yang disediakan oleh Windows 8 ini adalah *software based* artinya pengaturan DEP berbasiskan software. Sebenarnya beberapa prosesor komputer juga menyediakan *hardware-based DEP*. Di mana prosesor tersebut memakai teknologi hardware untuk mencegah program menjalankan kode program pada lokasi memori yang dilindungi (*protected memory*). Untuk mengetahui hal ini, bisa kita lihat pada tampilan depan *Data Execution Prevention*, seperti gambar di bawah ini terdapat pesan *Your computer's processor supports hardware-based DEP*.



Gambar 12.4 Informasi hardware-based DEP

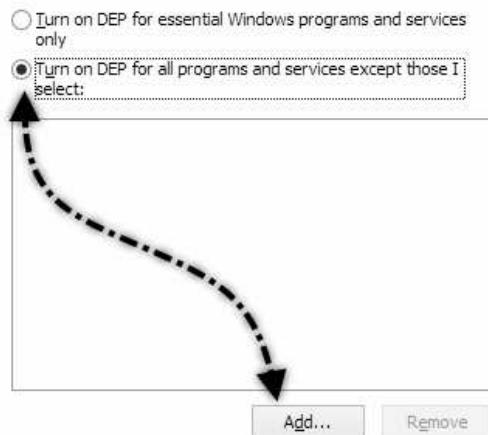
Apabila prosesor komputer Anda tidak mendukung hardware-based DEP maka pada bagian yang sama akan bertuliskan: "Your computer's processor does not support hardware-based DEP. However, Windows can use DEP software to help prevent some types of attacks".

12.1 Memasang Program pada Daftar DEP

Cara untuk menjalankan DEP telah dijelaskan sebelumnya, dari tampilan tersebut terdapat dua pilihan:

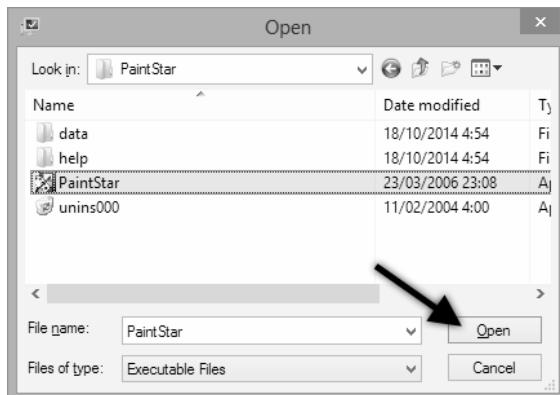
- *Turn on DEP for essential Windows programs and services only.* Pilihan ini akan membuat DEP melindungi program-program penting dan servis Windows.
- *Turn on DEP for essential Windows programs and services except those I select.* Pilihan ini akan membuat DEP melindungi seluruh program dan servis Windows kecuali program tertentu yang dipilih.

Sekarang kita pilih pilihan yang kedua, yaitu *Turn on DEP for essential Windows programs and services except those I select* maka tombol Add akan menjadi aktif. Untuk memasang program yang akan dilindungi atau dimatikan, klik tombol **Add** tersebut.



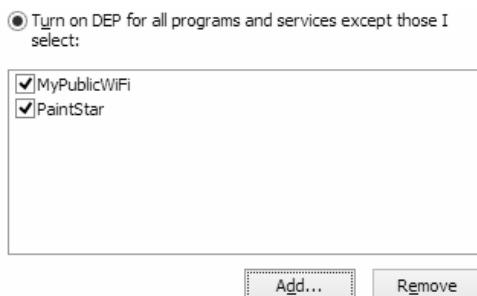
Gambar 12.5 Mengaktifkan DEP

Berikutnya akan tampil kotak dialog *Open* yang secara otomatis langsung membuka folder System32. Di dalamnya, kita bisa memilih program apa saja yang akan kita lindungi, atau Anda juga bisa mencari program di folder yang lainnya. Sebagai contoh saya memilih program yang bernama PaintStar. Klik pada nama program tersebut lalu klik tombol **Open**.



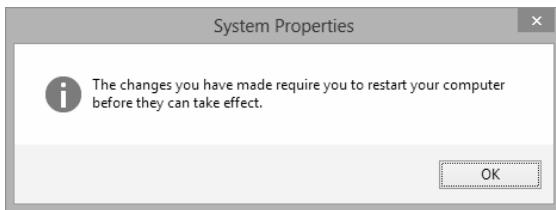
Gambar 12.6 Memilih program

Lakukan hal yang sama untuk program-program lainnya hingga masuk dalam daftar DEP. Di bawah ini saya telah memasukkan dua buah program.



Gambar 12.7 Daftar program

Daftar nama program yang diberi tanda centang berarti tidak dilindungi oleh DEP. Supaya program tersebut dilindungi maka hilangkan tanda centang pada nama program tersebut. Atau jika ada program yang ingin Anda keluarkan, klik pada nama program tersebut lalu klik tombol *Remove*. Setelah selesai Anda memasukkan nama program, klik tombol **OK**. Maka akan muncul pesan bahwa perubahan baru bisa diterapkan setelah Anda me-restart komputer. Klik saja tombol **OK**, dan **OK** sekali lagi sewaktu Anda kembali pada kotak dialog *System Properties*.



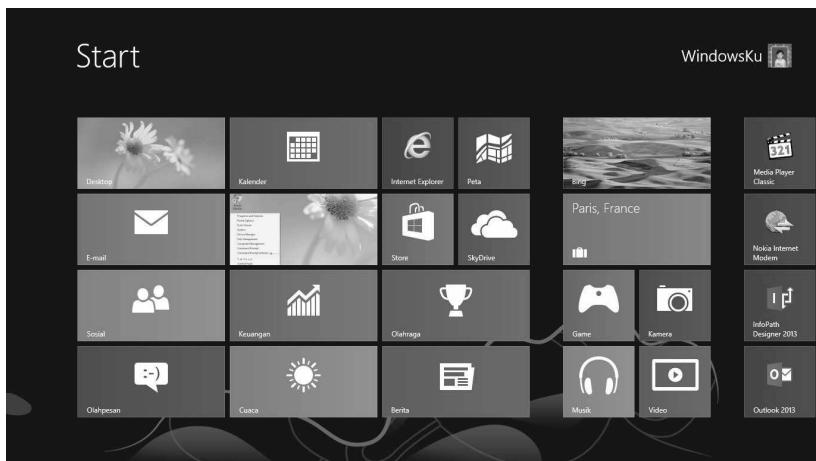
Gambar 12.8 Informasi restart

Sekarang restart-lah komputer Anda supaya perubahan yang Anda buat tersebut bisa diterapkan oleh Windows.

12.2 Mematikan DEP

Bila Anda merasa fitur DEP tidak begitu penting, atau terkadang malah mengganggu Anda maka Anda juga bisa mematikan DEP tersebut. Langsung saja, bukalah Command Prompt dengan status sebagai administrator. Cara menjalankan Command Prompt sebagai administrator adalah sebagai berikut:

1. Tampilkan halaman Start Windows.



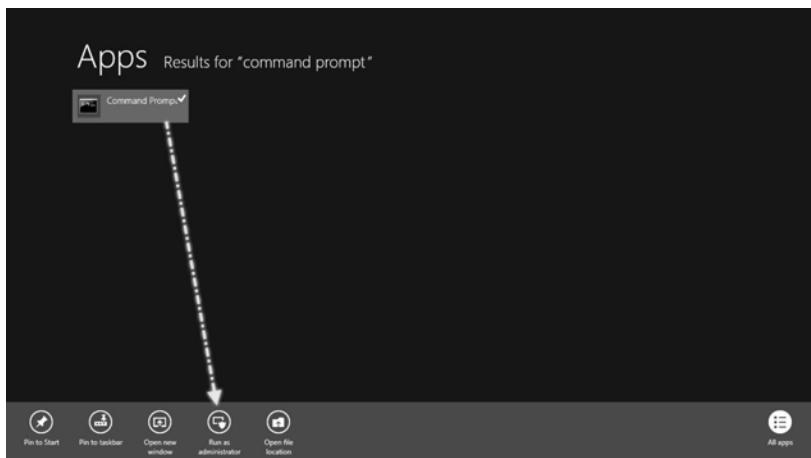
Gambar 12.9 Halaman Start

2. Dari tampilan di atas, ketik saja **command prompt**. Secara otomatis maka bagian *Search* dan apa yang Anda ketik akan tampil. Sedangkan pada sebelah kiri akan tampil program Command Prompt yang Anda ketik tersebut.



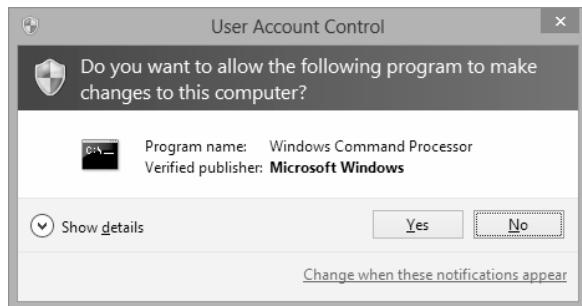
Gambar 12.10 Mengetik *command prompt*

3. Dari nama Command Prompt yang muncul di bawah tulisan *Apps*, lakukan klik kanan pada bagian tersebut. Secara otomatis program tersebut akan tercentang, sedangkan di bawahnya akan tampil berbagai pilihan. Klik pilihan **Run as administrator**.



Gambar 12.11 *Menu klik kanan*

4. Kemudian akan muncul kotak dialog konfirmasi, klik saja **Yes**.



Gambar 12.12 *User Account Control*

5. Dalam jendela kerja Command Prompt yang telah terbuka tersebut ketiklah: **bcdedit /set nx alwaysoff** kemudian tekan *Enter*.

A screenshot of an Administrator Command Prompt window. The title bar says "Administrator: Command Prompt". The window displays the following text:

```
Microsoft Windows [Version 6.2.9200]
(c) 2012 Microsoft Corporation. All rights reserved.

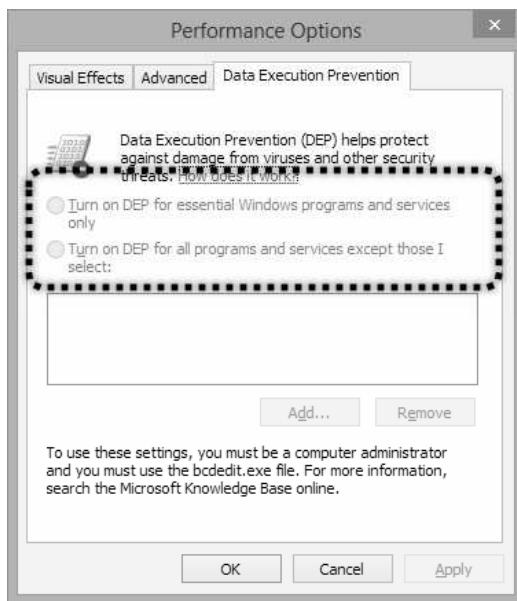
C:\Windows\system32>bcdedit /set nx alwaysoff
The operation completed successfully.

C:\Windows\system32>
```

Gambar 12.13 *Command Prompt*

6. Apabila pesan yang muncul bertuliskan *The operation completed successfully*, berarti proses yang Anda lakukan telah berhasil.

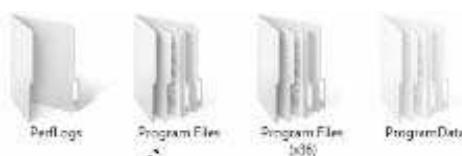
Untuk membuktikan apa yang telah Anda lakukan di atas, restartlah komputer terlebih dahulu. Setelah Windows kembali tampil, sekarang bukalah kotak dialog DEP maka akan terlihat seperti gambar di bawah ini. Pilihannya yang tersedia sebelumnya kini sudah tidak bisa digunakan lagi.



Gambar 12.14 Data Execution Prevention

12.3 Tips

Perlu diketahui juga bahwa fasilitas DEP tidak bisa digunakan pada program untuk Windows 8 yang 64-bit. Jadi, Anda harus mencari program-program yang 32 bit. Jika Anda menggunakan Windows 64-bit, untuk program yang 32-bit ditaruh dalam folder *Program Files (x86)*. Sedangkan program yang 64-bit disimpan dalam folder *Program Files*.

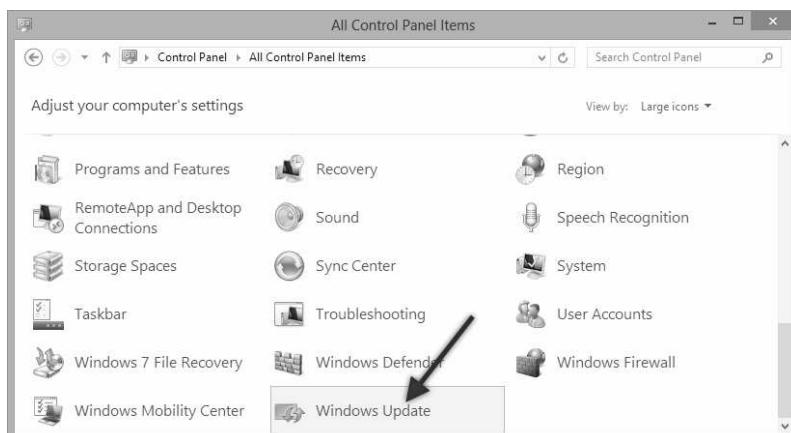


Gambar 12.15 Folder Program Files

13 PENTINGNYA WINDOWS UPDATE

Untuk meningkatkan keamanan Windows 8 maka sangat penting bagi kita untuk menjalankan Windows Update. Fitur ini akan melakukan pemeriksaan jika terdapat update untuk software dan juga driver dalam komputer. Tentu saja tujuannya untuk menambal apabila ada kelemahan dari program tersebut. Hasilnya tidak hanya keamanan Windows menjadi menjadi lebih kuat tetapi juga dari segi kinerja komputer akan menjadi lebih baik.

Untuk menjalankan fitur ini bisa diaktifkan dari Control Panel.



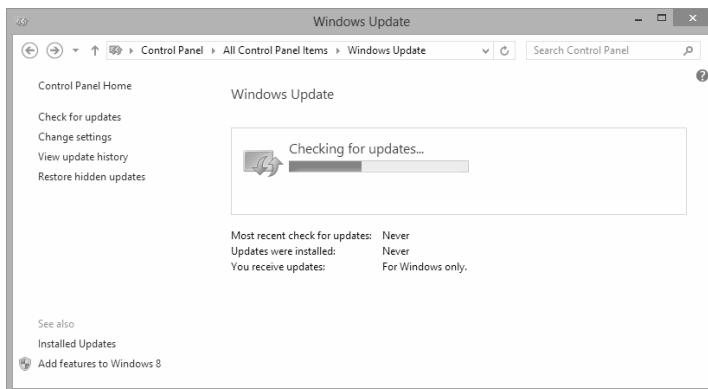
Gambar 13.1 Klik Windows Update

Secara default fitur ini sudah dalam kondisi aktif, namun apabila fitur ini tidak aktif maka Anda juga bisa melakukan update secara manual. Caranya adalah dengan menekan tombol **Check for updates** setelah Anda berada dalam halaman kerja Windows Update. Atau Anda juga bisa mengklik menu *Check for updates* yang berada pada panel sebelah kiri. Ingat, pastikan komputer Anda sedang terhubung ke internet untuk bisa melakukan pemeriksaan adanya update terbaru.



Gambar 13.2 Check for updates

Selanjutnya yang harus Anda lakukan adalah menunggu proses pemeriksaan update selesai dilakukan.



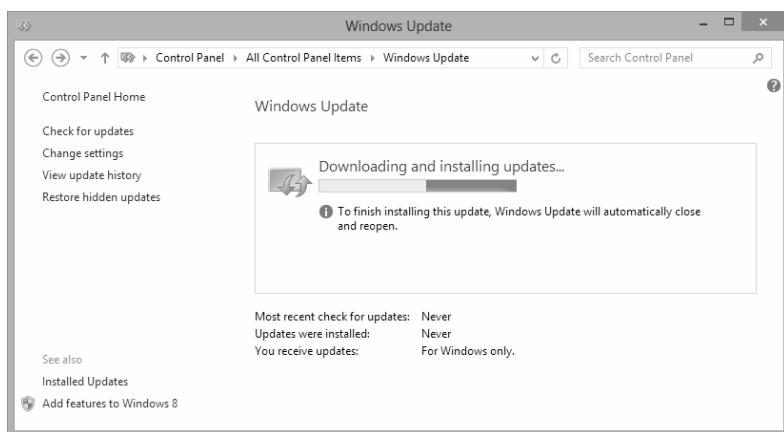
Gambar 13.3 Proses update

Setelah proses pemeriksaan update selesai dilakukan, klik tombol **Install now** untuk mendownload dan menginstall update terbaru tersebut.



Gambar 13.4 Install update

Semakin banyak update yang tersedia maka semakin lama proses download dan instalasi update yang dilakukan.



Gambar 13.5 Proses download dan install

Biasanya, setelah proses download dan install dilakukan, Anda disarankan untuk melakukan restart Windows.

Perlu Anda ketahui juga bahwa terdapat dua jenis update:

- *Important updates*: merupakan update untuk hal-hal yang penting dan kritis, seperti update untuk file sistem.
- *Recommended updates*: merupakan update tambahan yang disarankan oleh komputer. Update jenis kedua ini pada dasarnya tidak begitu utama, tapi terkadang juga diperlukan untuk meningkatkan keamanan komputer.

13.1 Memeriksa Status Windows Update

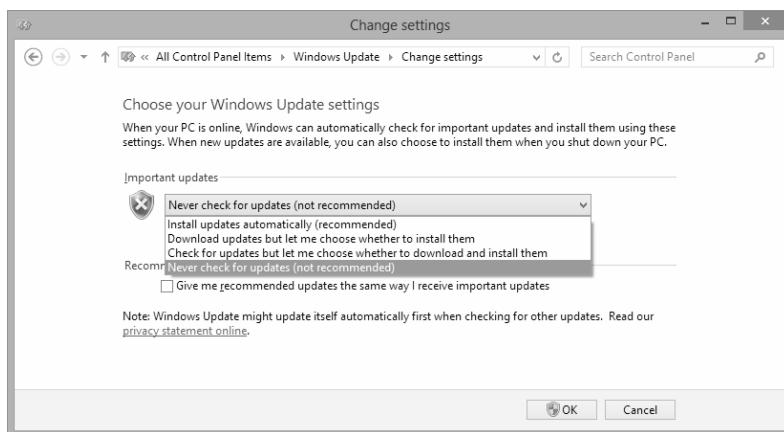
Walaupun fitur Windows Update ini secara default dalam kondisi aktif. Ada baiknya kita memeriksa untuk memastikannya, supaya komputer bisa melakukan proses update setiap kali komputer Anda terhubung ke internet.

Untuk memeriksa status Windows Update ini, klik menu **Change settings** yang berada pada panel sebelah kiri. Ada empat pilihan yang disediakan oleh Windows Update:

- *Install updates automatically (recommended)*: proses instalasi update dilakukan secara otomatis sewaktu Anda terhubung ke internet.
- *Download updates but let me choose whether to install them*: pilihan ini meminta Anda untuk memilih apakah Anda ingin menginstall update atau tidak setelah komputer men-download update terbaru.
- *Check for updates but let me choose whether to download and install them*: pilihan ini hampir sama dengan sebelumnya, hanya saja komputer cuma melakukan pemeriksaan apakah tersedia update yang baru atau tidak. Jika tersedia Anda diberi pilihan apakah ingin mendownload dan menginstallnya atau tidak. Perbedaan dengan pilihan sebelumnya adalah tidak dilakukannya proses download update terlebih dahulu.
- *Never check for updates (not recommended)*: pilihan yang terakhir ini tidak disarankan, yaitu Anda tidak ingin memeriksa apakah ada update terbaru atau tidak.

Pilihlah salah satu yang Anda rasa paling penting, terutama sekali bagi Anda yang memiliki koneksi internet unlimited sebaiknya memilih pilihan

pertama. Sedangkan kalau Anda memiliki koneksi internet yang tergantung pada quota maka pilihan kedua atau ketiga menjadi pilihan yang cocok bagi Anda. Setelah Anda memilih salah satu pilihan tersebut klik tombol **OK**.



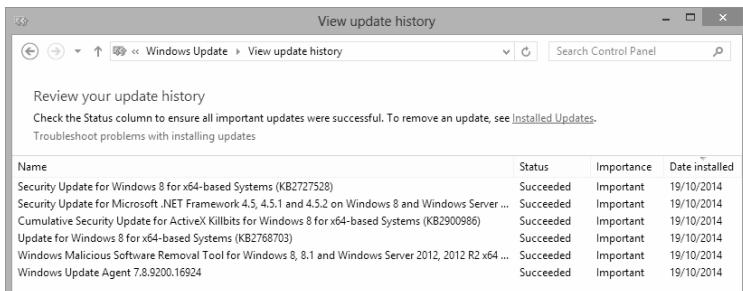
Gambar 13.6 Pilihan metode update

Selain memilih salah satu pilihan di atas, Anda juga bisa menentukan apakah akan melakukan hal yang sama untuk *Recommended updates*. Jika iya, Anda tinggal memberikan tanda centang pada bagian *Give me recommended updates the same way I receive important updates*.

13.2 Melihat History Update

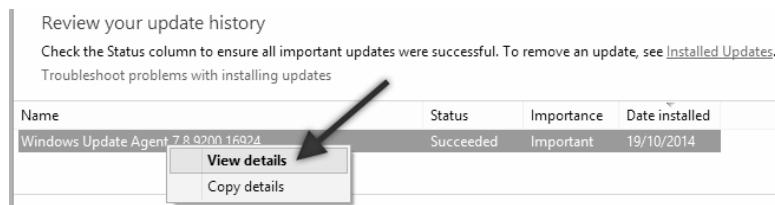
Selain mengetahui status program Windows Update, Anda juga bisa memeriksa atau mengetahui *history* atau update apa saja yang pernah dilakukan komputer. Informasi ini penting bagi kita untuk mengingatkan kembali mengenai update apa saja yang pernah kita lakukan terdahulu.

Untuk melakukan hal ini, klik pada **View update history** yang berada pada panel sebelah kiri. Di dalamnya, terdapat informasi mengenai update apa saja yang telah dilakukan oleh komputer Anda.



Gambar 13.7 History update

Untuk mengetahui informasi detail serta apa saja yang dilakukan oleh sebuah update, lakukan klik kanan pada nama update tersebut. Lalu dari menu yang muncul, klik **View Details**.

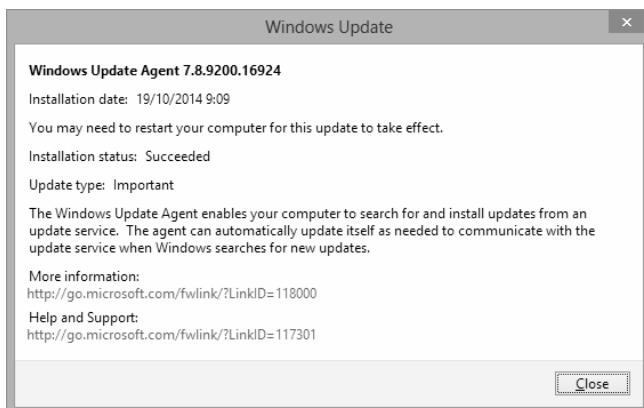


Gambar 13.8 Informasi detail update

Maka sebuah kotak dialog akan muncul, Anda bisa melihat informasi mengenai update tersebut. Sebagai contoh pada gambar di bawah ini terdapat informasi:

- Tanggal update dilakukan.
- Informasi bahwa untuk mengaktifkan update tersebut Anda diharuskan me-restart komputer terlebih dahulu.
- Status instalasi sukses.
- Jenis update: *Important*
- Ditampilkan juga sekilas informasi mengenai update tersebut dan juga link untuk melihat informasi lebih detail.

Terakhir untuk menutup kotak dialog tersebut, klik saja tombol **Close**.

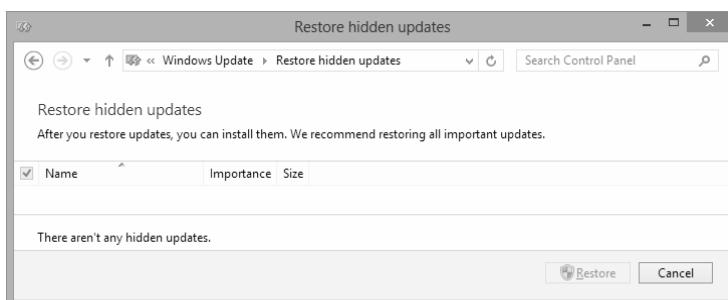


Gambar 13.9 Penjelasan mengenai update

13.3 Restore Hidden Update

Masih berhubungan dengan melihat history, kita juga bisa melihat update yang tidak diinstall. *Hidden update* merupakan update yang pernah kita tolak untuk tidak dilakukan proses instalasi. Semua update yang kita tolak tersebut disimpan pada bagian *Restore Hidden Update*.

Untuk melihat *hidden update* tersebut, klik link **Restore hidden updates**.



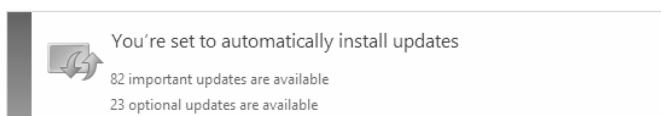
Gambar 13.10 Restore hidden updates

Kebetulan dalam komputer saya tidak terdapat *hidden update*, sehingga isinya kosong. Namun, apabila dalam komputer terdapat nama update

yang ingin Anda install, klik saja pada nama update tersebut dan klik tombol **Restore** supaya Windows menginstall update tersebut kembali.

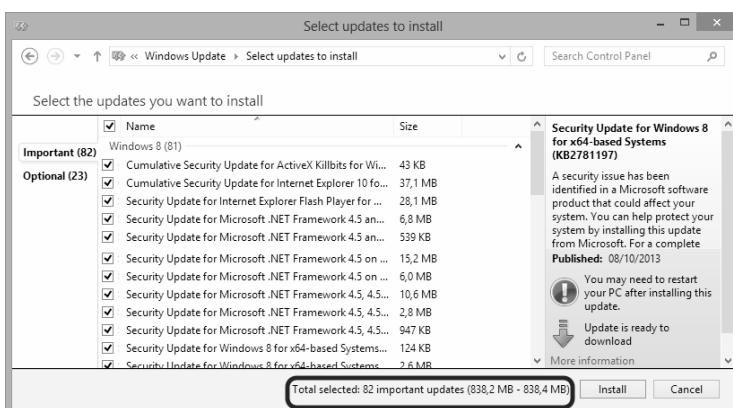
13.4 Memilih Update

Terkadang sewaktu Anda membuka Windows Update terdapat informasi mengenai jumlah update yang tersedia serta siap untuk di-download dan di-install. Misalnya, pada gambar di bawah ini terlihat ada 82 update penting yang tersedia (*important*), serta 23 update tambahan jika diperlukan (*optional*).



Gambar 13.11 Informasi update yang tersedia

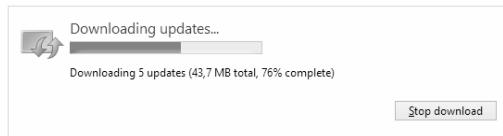
Dari gambar di bawah ini kita bisa melihat update apa saja yang akan dilakukan oleh Windows. Klik pada salah satu link tersebut untuk melihat update apa saja yang akan diinstal. Atau jika Anda merasa ada update yang tidak dibutuhkan maka Anda bisa menghilangkan tanda centang supaya tidak diinstall.



Gambar 13.12 Total update

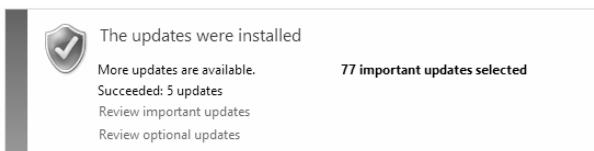
Pada kolom *Size* terdapat informasi berapa besar ukuran file yang akan di-download. Semakin banyak update yang Anda install maka semakin besar ukuran file-nya. Terakhir klik tombol **Install** untuk memulai proses download dan instalasi update.

Sebagai contoh untuk mempercepat proses maka saya hanya memilih lima update saja. Sekarang tungguah proses download update dilakukan sampai selesai.



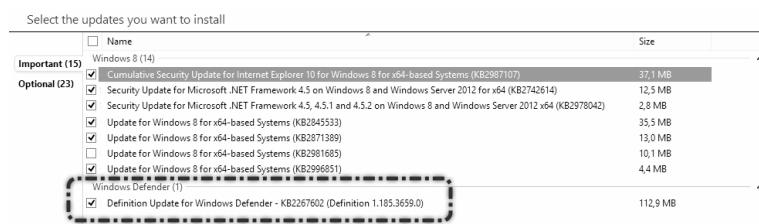
Gambar 13.13 Download update

Setelah selesai akan ditampilkan informasi bahwa 5 update berhasil diinstall.



Gambar 13.14 Update selesai

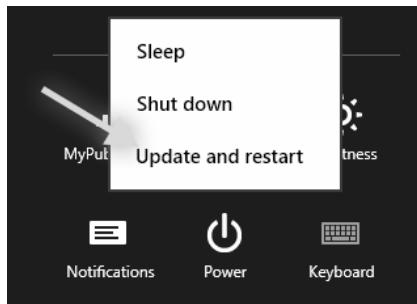
Perlu Anda ketahui bahwa Windows Update juga bisa memberikan informasi mengenai adanya update terbaru untuk Windows Defender. Sehingga kita bisa segera melakukan proses update Windows Defender.



Gambar 13.15 Update Windows Defender

13.5 Tips

Apabila dalam komputer Anda umumnya proses update dilakukan secara tersembunyi pada background tanpa sepengetahuan kita. Oleh karena kebanyakan proses instalasi memerlukan restart komputer maka salah satu cara untuk mengetahui apakah komputer Anda sudah mendownload dan menginstall update. Maka Anda bisa melihat pada menu *Power*, di mana pada bagian *Restart* kini berubah menjadi *Update and restart*. Hal ini berarti komputer telah melakukan update secara diam-diam (di *background*) sewaktu Anda terhubung ke internet. Setelah Anda melakukan restart komputer barulah update bisa berjalan dengan sempurna.



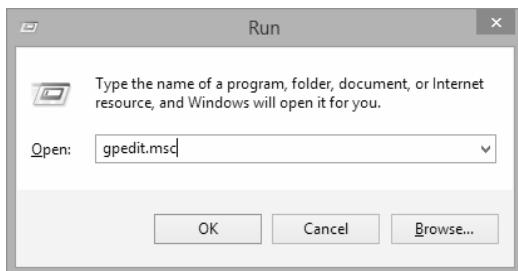
Gambar 13.16 *Update and restart*

14 LOCAL GROUP POLICY EDITOR

Local Group Policy Editor adalah sebuah *Microsoft Management Control (MMC)* dengan *user interface* yang mengizinkan semua objek *Local Group Policy* dikelola dari satu tempat. Di mana *Group Policy* itu sendiri adalah kebijakan atau semacam aturan untuk mengelola komputer serta pengaturan user.

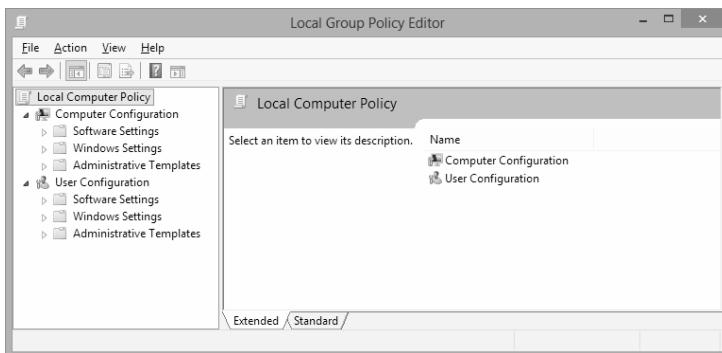
Untuk membuka Local Group Policy Editor, ikuti langkah berikut:

1. Buka kotak dialog *Run* dengan menekan kombinasi tombol keyboard, yaitu tombol **Windows** dan tombol **R** (**Win + R**). Tombol Windows adalah tombol pada keyboard yang berupa bendera atau logo Windows.
2. Dalam kotak dialog *Run* yang tampil, ketiklah **gpedit.msc** lalu klik **OK**.



Gambar 14.1 Kotak dialog Run

3. Maka akan tampil jendela kerja *Local Group Policy Editor*.



Gambar 14.2 *Local Group Policy Editor*

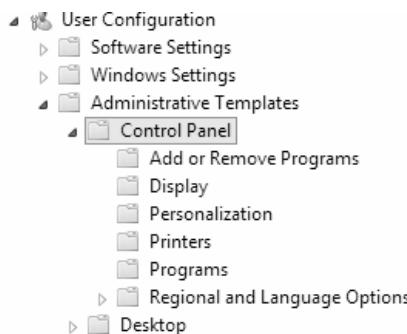
Dalam jendela kerja Local Group Policy Editor, terdapat dua bagian yang bisa kita atur, yaitu bagian *Computer Configuration* dan *User Configuration*. Kedua bagian tersebut memiliki konfigurasi untuk *Software Settings*, *Windows Settings*, dan *Administrative Templates*.

Pada dasarnya, ada banyak konfigurasi yang bisa kita atur dalam Local Group Policy Editor. Hanya saja kita tidak mungkin membahas semuanya karena bisa memakan satu buku tersendiri. Di sini saya hanya akan memberikan tiga contoh konfigurasi keamanan saja.

14.1 Melarang Akses Control Panel

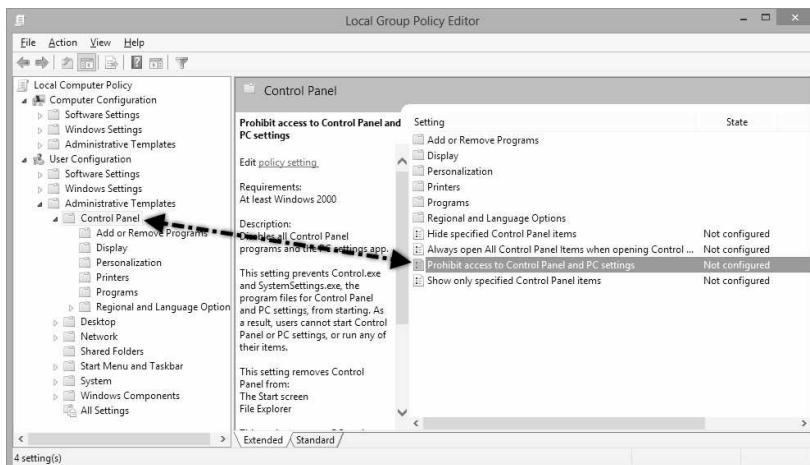
Seperti yang kita ketahui bahwa Control Panel merupakan lokasi sebagian besar pengaturan Windows berada. Sangat berbahaya sekali apabila ada orang yang tidak bertanggung jawab mengaksesnya. Kita bisa melarang akses ke Control Panel melalui Local Group Policy Editor.

Dalam jendela kerja Local Group Policy Editor, masuklah pada bagian **User Configuration** lalu klik dua kali pada **Administrative Templates**. Subfolder di bawahnya akan tampil, kali ini klik dua kali pada bagian **Control Panel**.



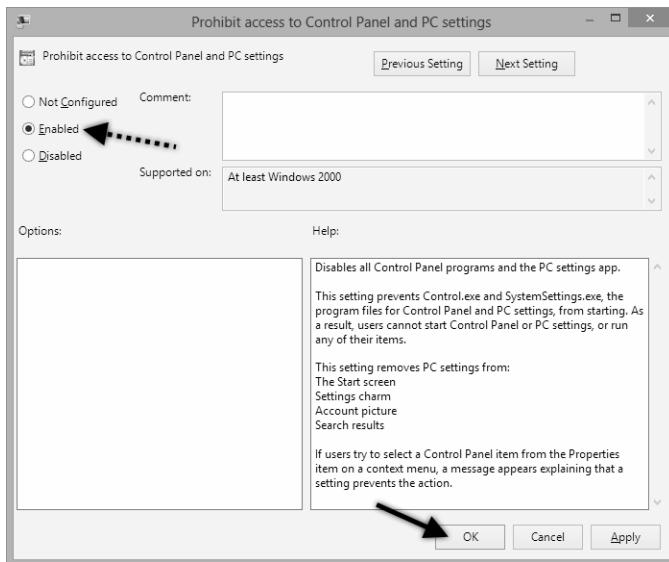
Gambar 14.3 Menu Control Panel

Selanjutnya perhatikan pada bagian yang sebelah kanan, carilah **Prohibit access to Control Panel and PC settings**, klik dua kali pada bagian tersebut.



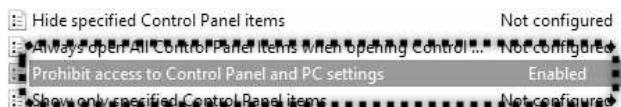
Gambar 14.4 Prohibit access to Control Panel and PC settings

Dari kotak dialog yang tampil berikan pilihan pada bagian **Enabled**. Setelah selesai klik **OK**.



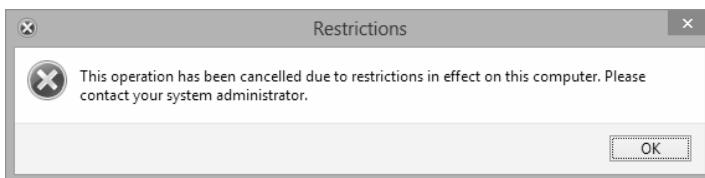
Gambar 14.5 Memilih Enabled

Sekembalinya Anda pada jendela kerja Local Group Policy Editor maka statusnya akan berubah menjadi *Enabled*.



Gambar 14.6 Status menjadi Enabled

Kini, Anda bisa mencoba membuka halaman Control Panel. Maka yang muncul adalah pesan larangan.



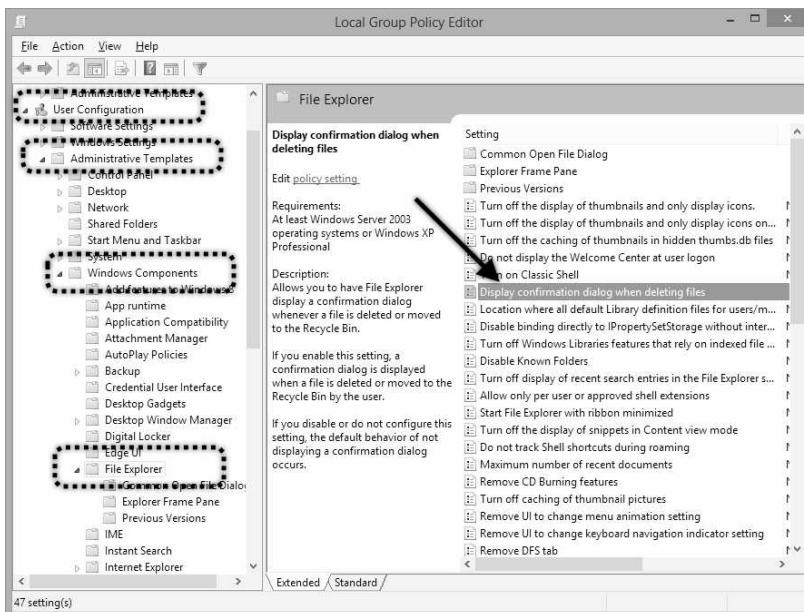
Gambar 14.7 Peringatan larangan akses

14.2 Menampilkan Konfirmasi Penghapusan

Secara default pada Windows 8, sewaktu kita akan menghapus sebuah file maka file tersebut akan langsung dimasukkan ke dalam Recycle Bin. Tindakan ini cukup berbahaya apabila kita secara tidak sengaja menekan tombol *Delete* pada keyboard.

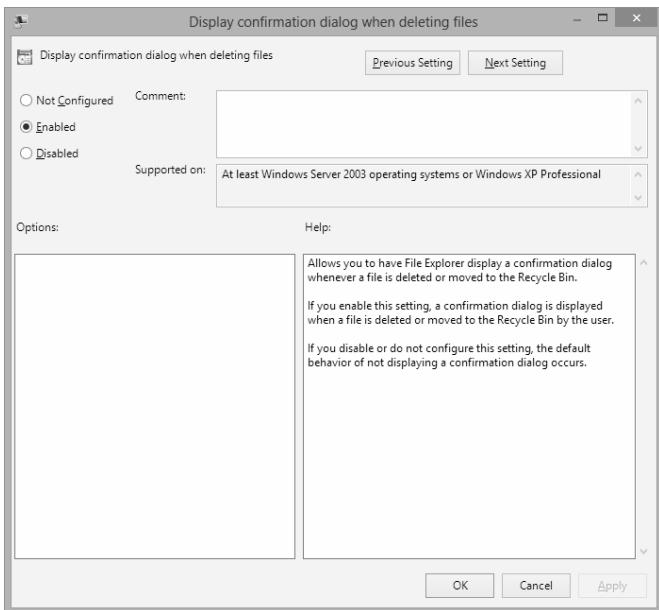
Dengan memanfaatkan Local Group Policy Editor, kita bisa menampilkan pesan konfirmasi sebelum sebuah file akan dimasukkan ke dalam Recycle Bin. Untuk melakukan hal tersebut, bukalah Local Group Policy Editor. Kemudian, tujulah pada bagian **User Configuration** lalu klik dua kali **Administrative Templates**.

Selanjutnya subfolder di bawahnya akan tampil, kali ini klik dua kali **Windows Components** lanjutkan pada bagian **File Explorer**.



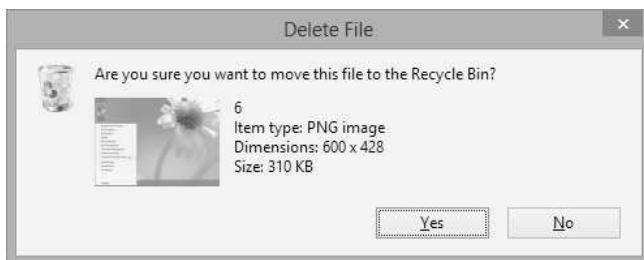
Gambar 14.8 Display confirmation dialog when deleting files

Terakhir klik dua kali pada **Display confirmation dialog when deleting files**, dan ubah pilihannya menjadi **Enabled**. Setelah selesai, klik **OK**.



Gambar 14.9 Memilih Enabled

Sekarang apabila Anda akan menghapus sebuah file atau folder maka akan ditampilkan kotak dialog konfirmasi apakah Anda benar-benar akan menghapus file tersebut atau tidak.



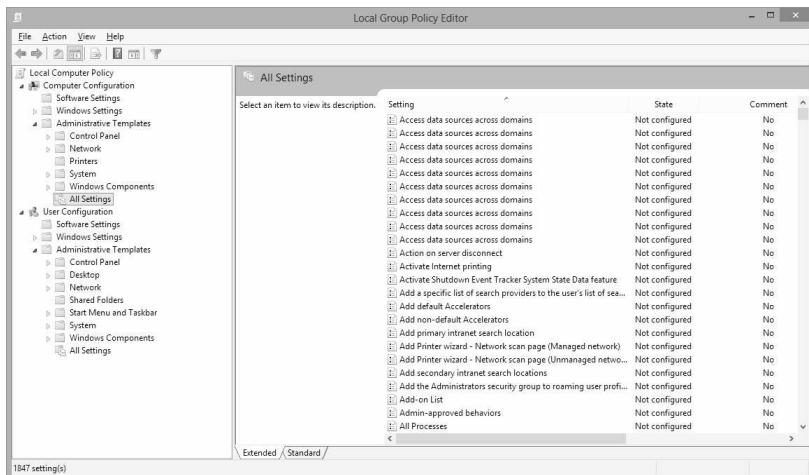
Gambar 14.10 Konfirmasi penghapusan file

Jika Anda mengklik Yes, barulah file tersebut akan dihapus atau dipindahkan ke dalam Recycle Bin. Seandainya Anda tidak sengaja menghapus atau tertekan tombol Delete kini Anda bisa memilih tombol /No untuk membatalkan aksi tersebut.

14.3 Menampilkan Seluruh Konfigurasi

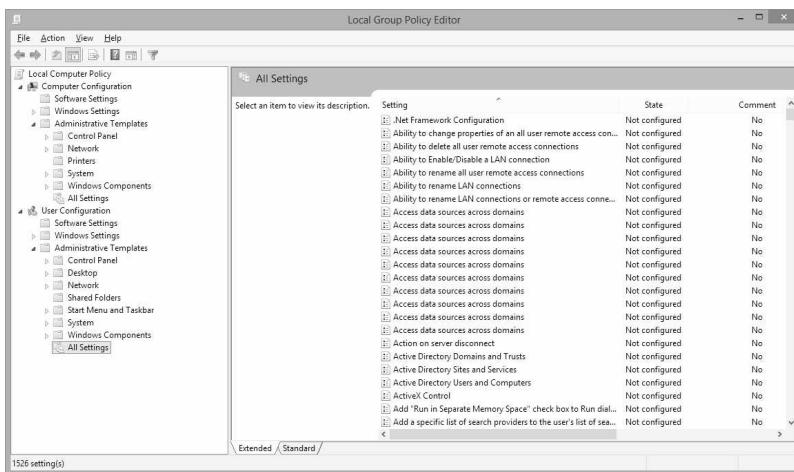
Sebelum meneruskan cara atau konfigurasi lainnya menggunakan Local Group Policy Editor. Saya akan menjelaskan terlebih dahulu mengenai cara menampilkan semua perintah yang terdapat dalam Local Group Policy Editor. Tujuannya supaya Anda tidak bingung jika harus mencari satu-persatu dalam setiap folder konfigurasi yang ada seperti dua contoh sebelumnya.

Untuk menampilkan semua konfigurasi dalam Local Group Policy Editor, perhatikan pada bagian **Administrative Tools** tepatnya pada bagian *Computer Configuration* maupun pada *User Configuration*. Jika Anda mengklik **All Settings** pada bagian *Computer Configuration* maka akan ditampilkan seluruh konfigurasi yang bisa Anda atur untuk *Computer Configuration*.



Gambar 14.11 Semua setting Computer Configuration

Lakukan hal yang sama untuk melihat seluruh konfigurasi pada bagian *User Configurations*.



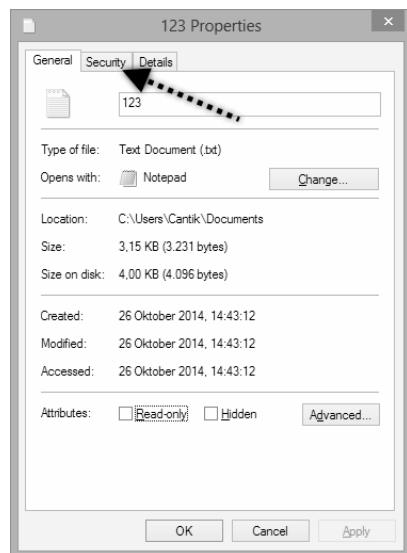
Gambar 14.12 Semua setting User Configuration

Dari kedua cara di atas kita tidak perlu lagi mencari konfigurasi dengan menelusuri folder satu persatu.

14.4 Menyembunyikan Tab Security

Setelah Anda melakukan langkah pada subbab sebelumnya, sekarang misalnya kita ingin menyembunyikan tab Security dalam kotak dialog *Properties* file atau folder. Tujuannya supaya orang lain tidak bisa mengubah setting keamanan data yang telah kita lakukan.

Sebelum meneruskannya, ada baiknya Anda melihat sebuah contoh kotak dialog *Properties* yang dalam kondisi normal terdapat sebuah tab *Security*. Tab itulah yang akan kita sembunyikan demi keamanan data.



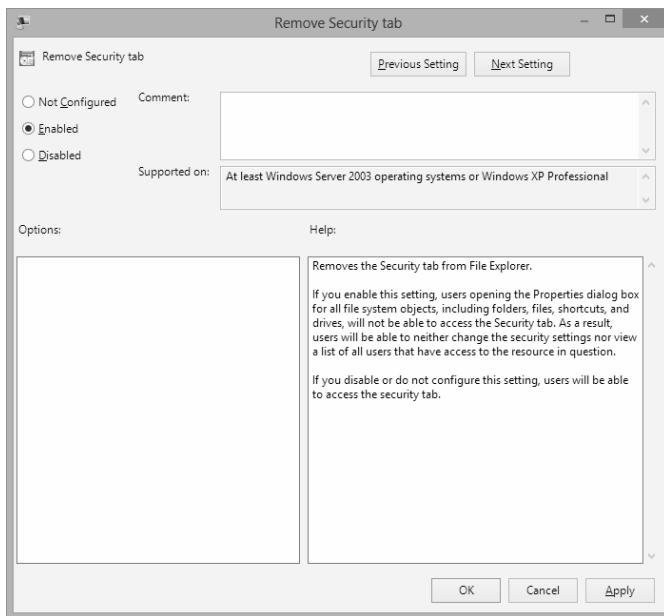
Gambar 14.13 Tab Security

Supaya prosesnya cepat, tampilkanlah semua konfigurasi pada bagian *User Configuration*. Setelah semua konfigurasi tampil, carilah **Remove Security tab**.

Setting	State	Comment
Remove Network Connections from Start Menu	Not configured	No
Remove Pictures icon from Start Menu	Not configured	No
Remove pinned programs from the Taskbar	Not configured	No
Remove pinned programs list from the Start Menu	Not configured	No
Remove pinned programs from File Explorer	Not configured	No
Remove Properties from the Computer icon context menu	Not configured	No
Remove Properties from the Documents icon context menu	Not configured	No
Remove Properties from the Recycle Bin context menu	Not configured	No
Remove Recent Items menu from Start Menu	Not configured	No
Remove See It Later / Search Everywhere link	Not configured	No
Remove Shared Folders from My Computer	Not configured	No
Remove Support Information	Not configured	No
Remove Task Manager	Not configured	No
Remove the 'Undock PC' button from the Start Menu	Not configured	No
Remove the Action Center icon	Not configured	No
Remove the battery meter	Not configured	No

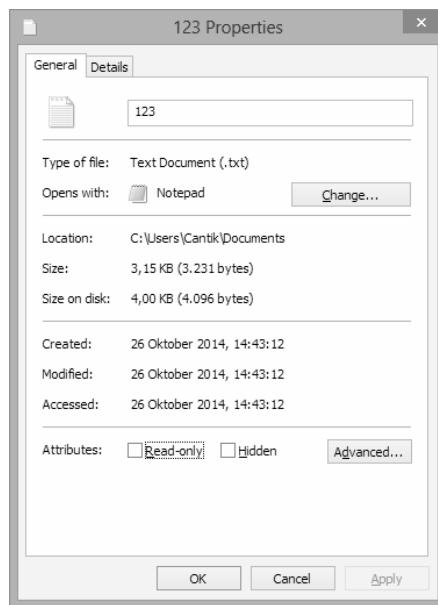
Gambar 14.14 Remove Security Tab

Klik dua kali pada bagian tersebut dan dalam kotak dialog yang tampil, berikan pilihan pada bagian **Enabled**. Terakhir klik **OK** untuk menerapkan perubahan.



Gambar 14.15 Memilih Enabled

Berikut contoh kotak dialog *Properties* yang tidak menampilkan tab *Security*.



Gambar 14.16 Tab Security telah hilang

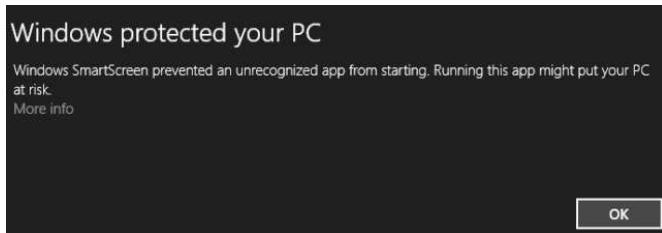
Sebagai penutup untuk bab ini, ada banyak setting lainnya yang bisa Anda coba satu-persatu. Selanjutnya saya persilahkan Anda untuk berekspresi dan mengeksplorasinya sendiri.

15 KONFIGURASI SMARTSCREEN

Selain dengan keberadaan Windows Defender dan Windows Firewall, dalam Windows 8 juga terdapat sebuah fitur keamanan lain yang bernama SmartScreen. SmartScreen merupakan fitur keamanan yang bekerja di-*background* komputer yang bertujuan untuk mencegah user menginstall dan menjalankan program berbahaya atau program yang tidak dikenal. Awalnya fasilitas SmartScreen ini hanyalah bagian dari Internet Explorer 8 dan 9, namun kini sudah diintegrasikan dengan Windows.

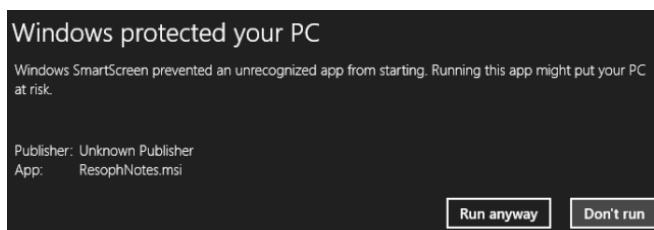
Secara default SmartScreen dalam kondisi aktif. Cara kerjanya adalah Windows 8 akan mengirim informasi untuk setiap aplikasi yang di download, ke server Microsoft yang kemudian akan diperiksa. Apabila program tersebut sah atau normal maka Windows 8 akan menjalankan program tersebut. Microsoft akan memeriksa program tersebut dengan membandingkan dengan data yang ada di-databasenya, jika tidak ditemukan dalam daftar yang tidak diizinkan maka program tidak akan dijalankan. Hal ini lebih ditujukan untuk mencegah program-program yang ada ditumpangi virus atau malware lainnya.

Pada saat Anda menjalankan program yang tidak dikenal oleh SmartScreen, maka akan tampil pesan yang mengatakan *Windows protected your PC*.



Gambar 15.1 Pesan perlindungan Windows

Masalahnya terkadang ada program yang baik-baik saja namun terdeteksi sebagai *unrecognized* atau tidak dikenal, pesan perlindungan tersebut akan selalu muncul. Hal ini cukup menjengkelkan. Jika Anda yakin dan percaya bahwa program yang Anda jalankan tersebut baik-baik saja, klik pada link **More info**. Maka akan tampil informasi mengenai program tersebut seperti di bawah ini.



Gambar 15.2 Informasi detail program

Jika Anda tetap nekat ingin menjalankan program tersebut, klik saja tombol **Run anyway**.

Bagi Anda yang merasa keberadaan SmartScreen ini cukup mengganggu sebenarnya Anda bisa menonaktifkan fasilitas ini. Namun, hal ini tidaklah disarankan.

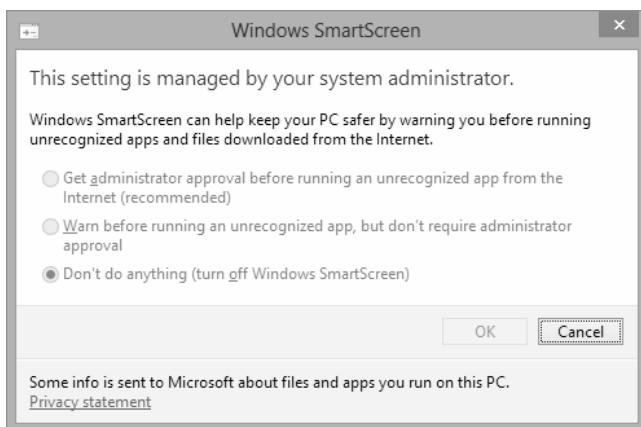
Kalau Anda masih keras kepala untuk mengetahui cara menonaktifkan SmartScreen ini, ikuti langkah berikut:

1. Masuklah ke dalam Control Panel, lalu jalankan **Action Center**.
2. Dari jendela kerja *Action Center*, perhatikanlah pada panel sebelah kiri, klik **Change Windows SmartScreen settings**.



Gambar 15.3 Change Windows SmartScreen settings

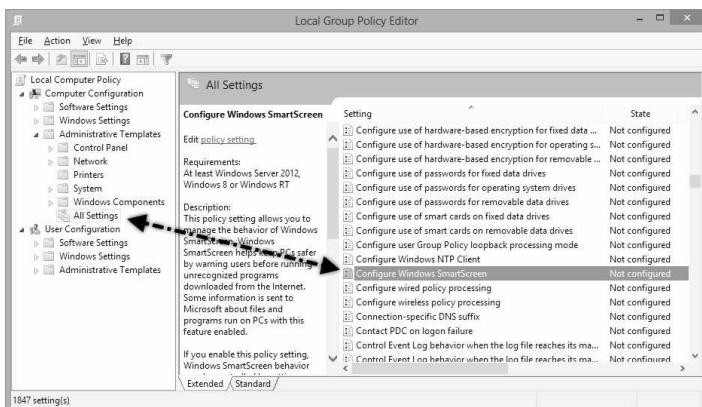
3. Selanjutnya akan tampil kotak dialog *Windows SmartScreen*.



Gambar 15.4 Windows SmartScreen

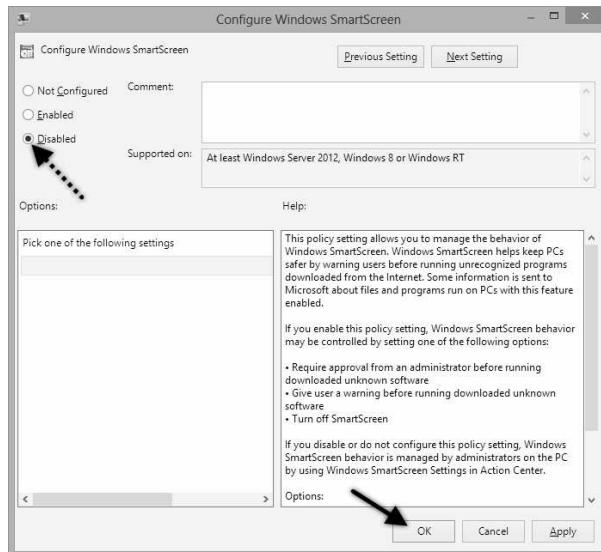
Masalahnya adalah Anda tidak bisa melakukan konfigurasi apapun di dalamnya. Anda tidak dapat mengaktifkan termasuk juga menonaktifkan pilihan yang tersedia. Untuk mengatasi hal di atas, ikuti langkah berikut:

1. Masuklah ke dalam jendela kerja *Local Group Policy Editor* seperti yang dijelaskan dalam bab sebelumnya.
2. Tujulah pada bagian berikut: Computer Configuration > Administrative Templates > All Settings
3. Sedangkan di panel sebelah kanan, carilah **Configure Windows SmartScreen**. Setelah ditemukan, klik dua kali pada bagian tersebut.



Gambar 15.5 Configure Windows SmartScreen

4. Kotak dialog *Configure SmartScreen* akan tampil. Kemudian pilihlah *Disabled* dan klik tombol **OK**.



Gambar 15.6 Memilih Disabled

Terakhir buka kembali kotak dialog *Windows SmartScreen* dari Action Center. Sekarang semua pilihannya sudah bisa digunakan.



Gambar 15.7 Opsi Windows SmartScreen telah aktif

Aturlah pilihan *SmartScreen* sesuai dengan yang Anda inginkan:

- *Get administrator approval before running an unrecognized app from the Internet (recommended).* Ini adalah pilihan yang direkomendasikan oleh Windows, di mana setiap program yang tidak dikenal harus melalui persetujuan administrator sebelum dijalankan.
- *Warn before running an unrecognized app, but don't require administrator approval.* Pilihan yang kedua ini hanya memberi pesan peringatan tidak memerlukan persetujuan administrator untuk menjalankan program yang tidak dikenal.
- *Don't do anything (turn off Windows SmartScreen).* Pilihan ini adalah untuk mematikan fasilitas SmartScreen.

Pilihlah salah satu yang ingin Anda gunakan lalu klik **OK**.

16 TRIK KEAMANAN TAMBAHAN

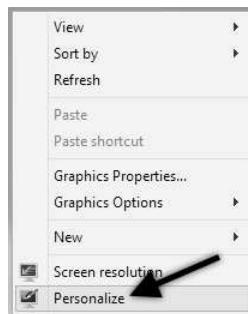
Dalam bab ini, akan dijelaskan berbagai pengaturan keamanan tambahan yang terdapat dalam Windows 8 dan juga Windows 8.1. Pengaturan keamanan di sini sengaja saya pisahkan karena tidak dapat saya kelompokkan pada bab-bab terdahulu.

16.1 Screen Saver Sebagai Pengaman

Tatkala Anda sedang mengetik dan tiba-tiba harus menggunakan komputer maka yang umum digunakan oleh user adalah mengaktifkan screen saver. Dan sebenarnya, screen saver tersebut juga bisa kita manfaatkan sebagai pengamanan tambahan dalam komputer kita. Sebab, ketika Anda kembali untuk menggunakan komputer maka Windows mewajibkan Anda untuk memasukkan password terlebih dahulu. Namun, pastikan komputer Anda telah menggunakan password terlebih dahulu.

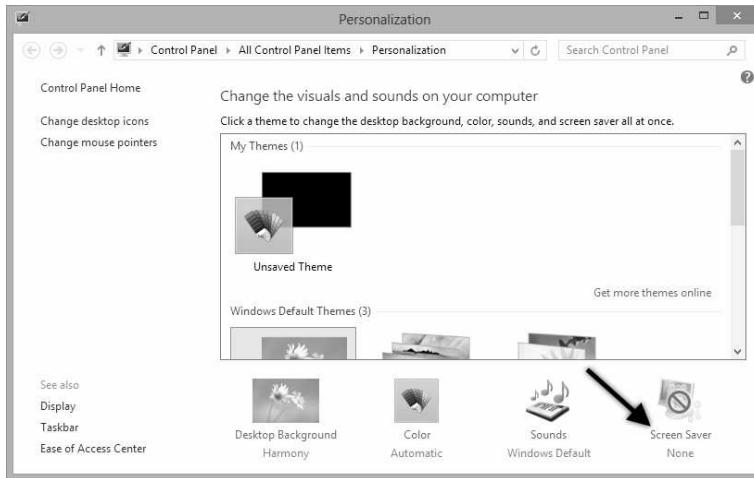
Untuk menggunakan screen saver sebagai pengamanan tambahan adalah sebagai berikut:

1. Klik kanan pada dekstop (halaman muka) komputer Anda, dan dari menu yang muncul klik **Personalize**.



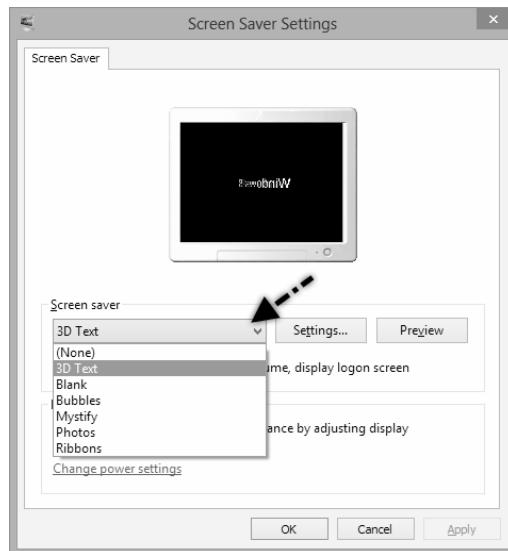
Gambar 16.1 Menu klik kanan desktop

2. Dari jendela kerja *Personalization* yang muncul klik pada menu **Screen Saver** yang terdapat pada bagian kanan bawah.



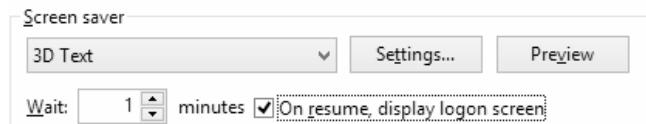
Gambar 16.2 Personalization

3. Selanjutnya akan tampil kotak dialog *Screeen Saver Settings*. Dalam kotak dialog tersebut pilihlah model screen saver yang Anda inginkan dengan mengklik *drop down list*. Sebagai contoh pada gambar di bawah ini saya memilih *3D Text*.



Gambar 16.3 Memilih Screen saver

4. Kemudian atur waktu berapa menit tunggu sebelum screen saver tampil.
5. Dan yang paling penting adalah memberikan tanda centang pada bagian **On resume, display logon screen**.



Gambar 16.4 On resume, display logo screen

6. Setelah semua langkah di atas selesai Anda lakukan klik **OK**.

Sebagai terlihat pada gambar di atas, saya mengatur waktu untuk screen saver selama satu menit. Berarti, jika dalam satu menit tidak ada aktivitas pada komputer saya maka screen saver akan aktif. Dan apabila saya ingin menggunakan kembali komputer maka tampilan yang pertama kali muncul adalah *logon screen* yang mewajibkan kita untuk memasukkan password.

16.2 Safe Mode pada Windows 8

Tidak seperti pendahulunya, di mana seseorang bisa login Windows dalam Safe Mode hanya dengan menekan tombol F8 pada keyboard secara berulang kali. Cara seperti itu tidak berlaku untuk Windows 8. Oleh karena itu, perlu sedikit trik tambahan yang harus Anda lakukan. Sebelum menjelaskan bagaimana kita bisa masuk dalam Safe Mode pada Windows 8. Ada baiknya, saya jelaskan sedikit mengenai apa itu Safe Mode.

Safe Mode adalah salah satu metode untuk login dalam Windows. Hanya saja pada Safe Mode ini akan menjalankan Windows dengan driver dan servis dan driver yang standard saja. Dengan kondisi Windows yang menjalankan sedikit servis dan driver maka Safe Mode bisa dimanfaatkan untuk melakukan *troubleshooting* apabila ada masalah dengan Windows. Misalnya, Windows kita memiliki masalah jika di-load dengan kondisi normal. Namun ketika menggunakan Windows dengan Safe Mode masalah tersebut tidak muncul maka bisa diasumsikan bahwa masalah tersebut bukanlah berasal dari driver maupun dari setting default Windows. Bisa saja penyebabnya adalah dari program yang baru saja kita install, atau dari driver perangkat baru yang kita pasang.

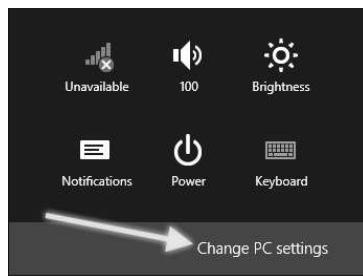
Baiklah, ikuti langkah berikut untuk menjalankan Windows 8 dalam Safe Mode:

1. Tampilkanlah menu pada bagian kanan layar monitor Anda dengan cara mengarahkan mouse pada sudut kanan atas. Dari pilihan yang muncul, geserlah mouse ke bawah dan klik **Settings**.



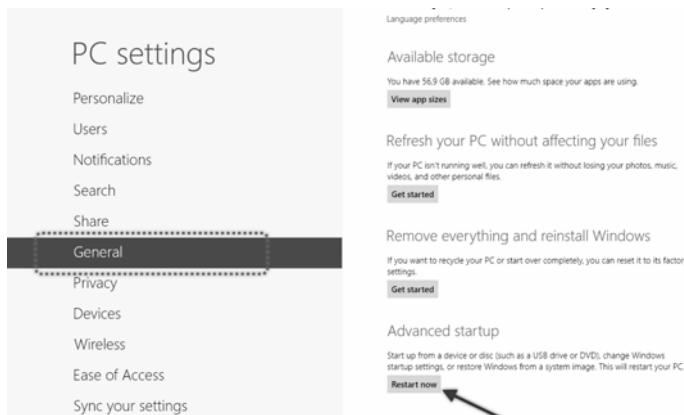
Gambar 16.5 Klik **Settings**

2. Dari pilihan *Settings* yang muncul, klik pada tulisan di bagian bawah yang bertuliskan **Change PC Settings**.



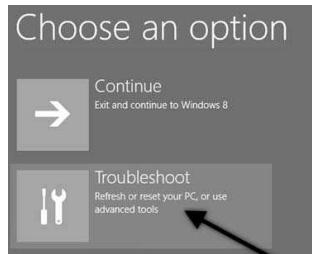
Gambar 16.6 Klik *Change PC settings*

3. Selanjutnya pada tampilan *PC settings*, pada panel sebelah kiri, klik **General**. Sedangkan isinya di sebelah kanan scroll ke bagian paling bawah, tepatnya pada tulisan *Advanced startup*. Klik tombol **Restart now**.



Gambar 16.7 Gambar 16.8 *PC settings*

4. Kini, komputer Anda akan bersiap melakukan restart. Pada tampilan berikutnya, kita dihadapkan pada beberapa pilihan, klik **Troubleshoot**.



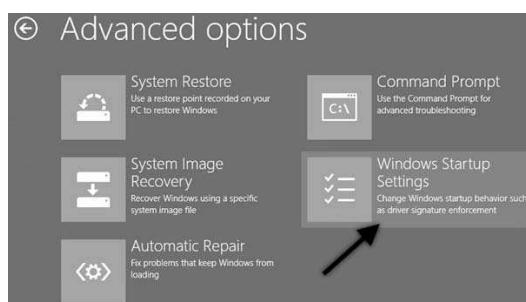
Gambar 16.8 Klik Troubleshoot

5. Selanjutnya, dari pilihan **Troubleshoot**, klik pada bagian **Advanced options**.



Gambar 16.9 Klik Advanced options

6. Setelah itu, akan tampil beberapa opsi, klik **Windows Startup Settings**.



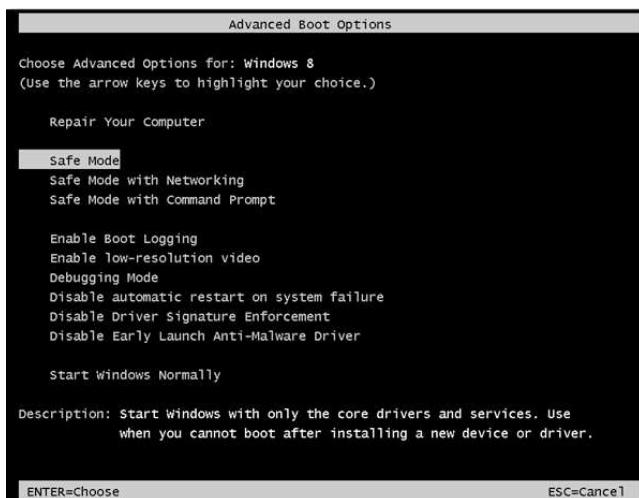
Gambar 16.10 Klik Windows Startup Settings

7. Informasi mengenai setting startup segera tampil, sekarang klik tombol **Restart**.



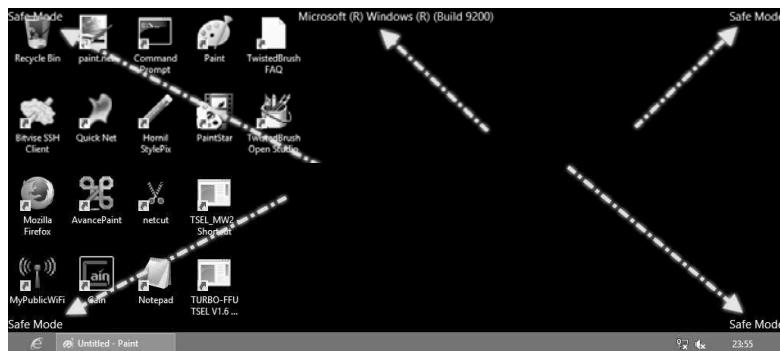
Gambar 16.11 Klik Restart

8. Setelah komputer restart maka akan tampil beberapa pilihan yang bisa Anda gunakan. Pilihlah **Safe Mode**. Anda bisa menggunakan tanda panah pada keyboard untuk memilih salah satu pilihan, setelah sampai pada bagian *Safe Mode*, tekan tombol **Enter** pada keyboard.



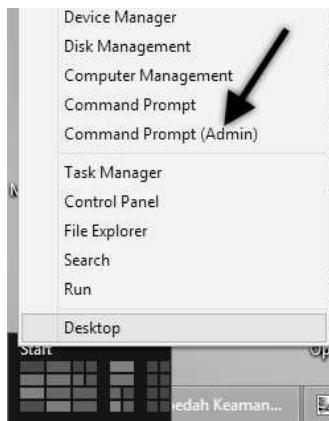
Gambar 16.12 Advanced Boot Options

Berikut contoh tampilan Windows ketika berada dalam Safe Mode maka pada setiap sudut akan terdapat teks bertuliskan *Safe Mode*.



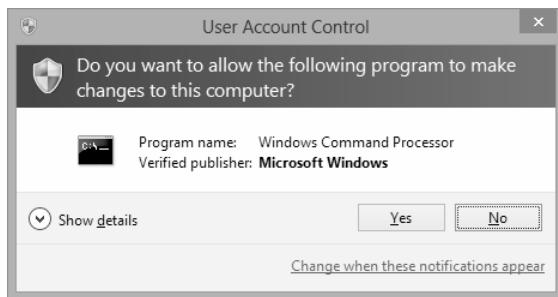
Gambar 16.13 *Safe Mode*

Sebagai tambahan, apabila Anda tidak ingin melakukan langkah di atas secara berulang-ulang untuk masuk dalam kondisi Safe Mode. Anda juga bisa membuat supaya Safe Mode bisa bekerja dengan menekan tombol F8 seperti Windows versi sebelumnya. Caranya adalah dengan membuka Command Prompt dengan modus administrator, yaitu dengan mengklik kanan pada sudut kiri bawah halaman komputer Anda. Dan dari menu yang muncul klik **Command Prompt (Admin)**.



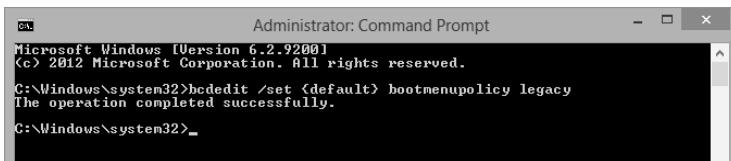
Gambar 16.14 *Menu klik kanan sudut kiri bawah*

Apabila muncul kotak dialog *User Account Control*, klik **Yes**.



Gambar 16.15 *User Account Control*

Setelah Anda berada dalam jendela kerja Command Prompt, ketiklah perintah berikut: **bcdedit /set {default} bootmenupolicy legacy** lalu tekan *Enter*. Maka akan tampil pesan *The operation completed successfully*, hal ini berarti pemberian perintah yang kita berikan telah berhasil dilakukan. Perhatikan contohnya pada gambar di bawah ini.



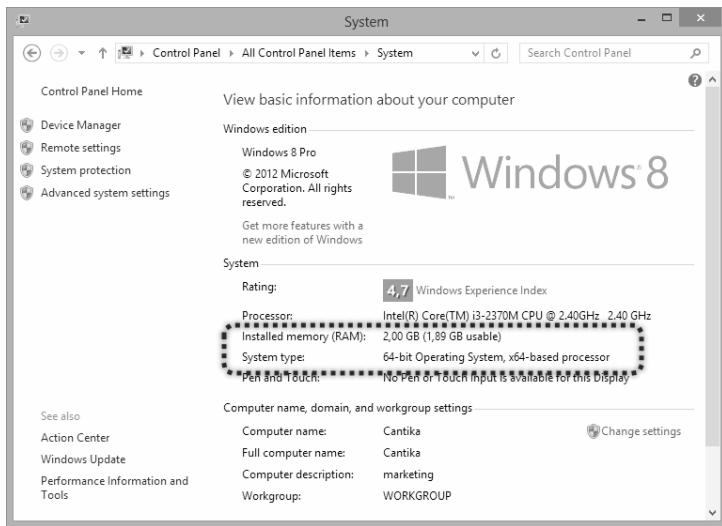
Gambar 16.16 *Command Prompt*

Selanjutnya, Anda bisa login ke dalam Windows dengan menekan tombol F8 pada keyboard sewaktu booting. Menu pilihan untuk masuk ke dalam Windows dengan pilihan Safe Mode akan tampil.

16.3 Mencari Versi Windows

Banyak di antara pengguna komputer yang sudah sering menggunakan komputer tapi tidak pernah tahu berapa bit versi Windows yang digunakan. Tanpa banyak basa-basi lagi untuk mengetahui berapa bit versi Windows yang Anda gunakan. Masuklah ke dalam Control Panel, dan klik dua kali pada ikon **System**.

Dari jendela kerja *System* yang tampil perhatikan pada bagian *System type*. Di sanalah informasi berapa bit Windows yang Anda gunakan. Pada gambar di bawah ini terlihat kalau komputer saya menggunakan Windows 8 versi 64-bit.



Gambar 16.17 Informasi sistem

16.4 Mencegah Penularan Virus

Dari penjelasan terdahulu virus memang menjadi salah satu perhatian dalam masalah keamanan. Kita telah membicarakan mengenai Windows Defender dan juga DEP. Belum lagi dari pemeriksaan servis siapa tahu ada virus yang jalan secara diam-diam di-*background*.

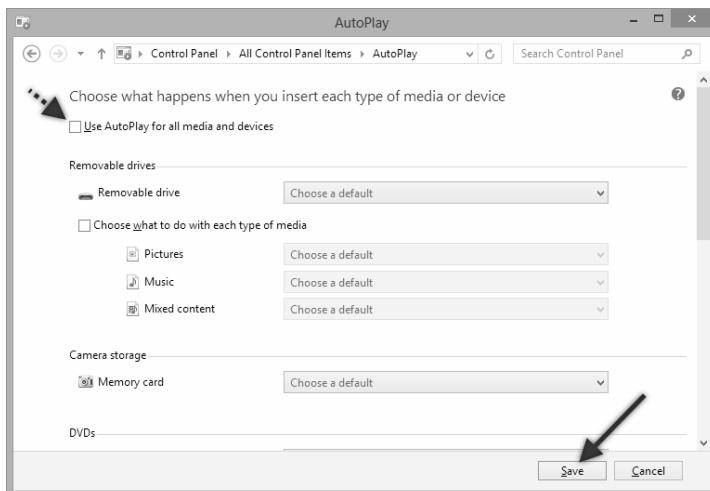
Sebagaimana yang kita ketahui bahwa salah satu sarana untuk penularan virus selain internet, adalah dari pemakaian flashdisk. Khusus dalam subbab ini, kita akan menjelaskan cara mencegah penularan virus melalui media flashdisk, termasuk juga CD.

Untuk melakukan trik ini, bukalah Control Panel, kemudian jalankan ikon **AutoPlay**.



Gambar 16.18 Ikon AutoPlay

Dalam jendela kerja *AutoPlay*, sebenarnya terdapat cukup banyak pengaturan yang bisa Anda lakukan. Misalnya, bagaimana kalau yang kita sisipkan adalah Memory Card kamera digital, CD Audio dan sebagainya. Namun, akan sangat baik sekali Anda mematikan fasilitas *Autoplay* ini dengan menghilangkan tanda centang pada bagian **Use AutoPlay for all media and devices**. Terakhir klik tombol **Save** untuk menyimpan perubahan.



Gambar 16.19 AutoPlay

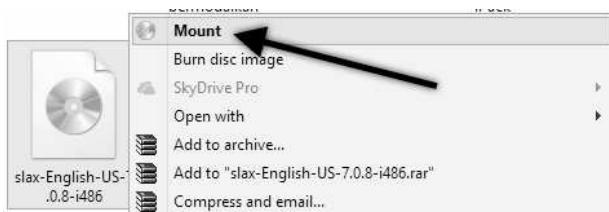
Fungsinya adalah untuk mencegah menyedia penyimpanan apapun, seperti flashdisk yang ketika dipasang langsung aktif menjalankan sebuah program (*Autorun*).

16.5 Virtual Drive

Apabila Anda memiliki file cadangan (backup) yang disimpan dalam bentuk file ISO atau yang sejenisnya (*.nrg). Dengan adanya Windows 8

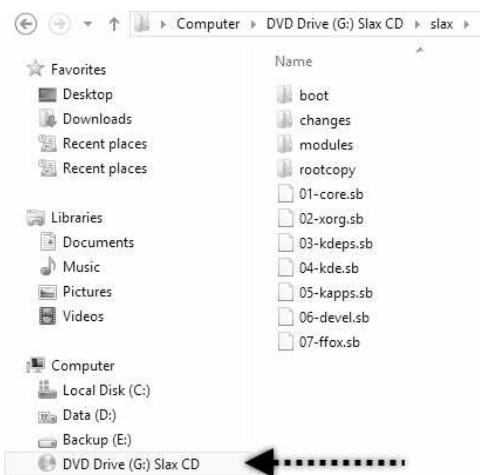
maka Anda tidak perlu menginstall program pihak ketiga. Karena dalam Windows 8 sudah tersedia sebuah fasilitas Virtual Drive secara *native*.

Cara penggunaanya juga sangat mudah sekali, kita hanya perlu melakukan *double click* pada file iso tersebut maka Windows secara otomatis akan melakukan *mount*. Kita juga bisa melakukan klik kanan dan klik menu *mount*. Untuk lebih jelasnya, perhatikan contoh di bawah ini. Sebuah file iso yang kita klik kanan maka akan tampil beberapa menu, lalu klik **mount**.



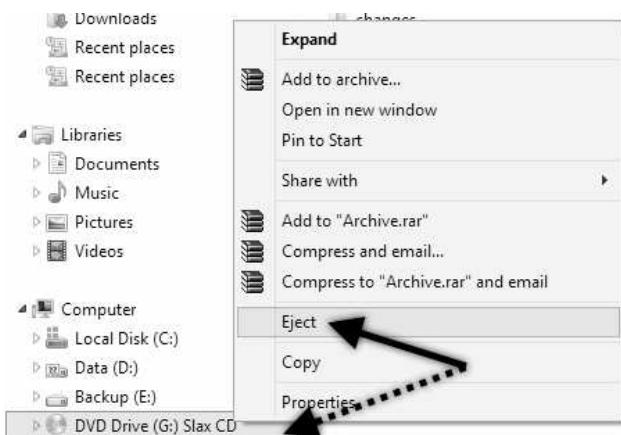
Gambar 16.20 Menu klik kanan file ISO

Secara otomatis sebuah drive baru akan muncul, sesuai dengan nama file iso tersebut. Dan di sebelah kanannya kita dapat melihat isi dari file iso tersebut.



Gambar 16.21 Drive virtual

Jika Anda sudah selesai menggunakan file iso maupun virtual drive tersebut. Lakukan klik kanan pada drive virtual tersebut dan klik **Eject** maka file iso tersebut akan di-unmount. Begitu pula dengan drive virtual tersebut akan hilang.



Gambar 16.22 Klik Eject

Kini Anda sudah memiliki sebuah drive virtual yang mudah dan murah tanpa harus menginstall program pihak ketiga lagi.

TENTANG PENULIS

Vyctoria adalah media content provider yang bergerak di bidang penulisan buku-buku bertemakan komputer dan teknologi informasi. Vyctoria hingga saat ini telah banyak mengulas berbagai tema IT yang menarik namun jarang diulas dan akan terus mengeluarkan berbagai buku-buku komputer yang unik lainnya. Buku-buku lain yang telah diterbitkan oleh Vyctoria bisa Anda lihat di <http://www.vyctoriaku.com>

Dapat dihubungi melalui email: vyctoriaku@gmail.com

Catatan:

Untuk melakukan pemesanan buku, hubungi

Layanan Langsung PT Elex Media Komputindo: Gramedia Direct

Jl. Palmerah Barat No. 29-37, Jakarta 10270

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

Email: endang@gramediapublishers.com

Tips & Trik Keamanan Windows 8 & 8.1



Dalam Windows 8 dan Windows 8.1 ada banyak sistem keamanan yang telah disediakan. Namun, apabila kita tidak bisa menggunakananya secara optimal, tentu saja semua fasilitas tersebut terbengkalai dan menjadi pajangan saja.

Buku ini menyajikan berbagai tips dan trik seputar sistem keamanan Windows 8 dan Windows 8.1. Isinya adalah langkah-langkah praktis untuk menggunakan dan mengoptimalkan fitur keamanan yang tersedia.

Selengkapnya, buku ini mencakup:

- Mengelola user accounts
- Microsoft account
- Password reset disk
- Family safety & event viewer
- Keamanan file dan folder
- Windows defender
- Windows firewall
- File history
- Recovery
- System configuration
- Data execution prevention
- Windows update
- Local group policy editor
- Konfigurasi smartscreen
- Trik keamanan tambahan

PT ELEX MEDIA KOMPUTINDO
Kompas Gramedia Building
Jl. Palmerah Barat 29-37, Jakarta 10270
Telp. (021) 53650110-53650111, Ext 3214
Webpage: <http://www.elexmedia.co.id>

gramedia

Kelompok
Sistem Operasi
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 978-602-02-5475-3

9 78602 0254753
121142602