# Aplikasi Pada Struktur Registry Windows

**Moch Yusup Soleh**
Program Studi Teknik Informatika ITB
Jl Ganesha no 10 Bandung, email: if17051@students.itb.ac.id

***Abstract –*** *Makalah ini menjelaskan tentang windows registry sebagai aplikasi dari beberapa bab yang telah dipelajari pada mata kuliah struktur diskrit ITB, mulai dari logika, himpunan serta pohon.*

***Kata Kunci****: Struktur, Pohon, Logika, Himpunan .*

## 1. PENDAHULUAN

*Windows registry* adalah sebuah data base yang disusun secara hirarki yang mengandung nilai dari variabel-variabel di dalam *Windows* dan di aplikasi dan *Services* yang berjalan di *Windows*. Tidak hanya itu, operating Sistem dan program-program lain pun menyimpan data dari user-usernya dan tentang konfigurasi sistem beserta komponen-komponennya didalam registry. Karena registry selalu tersedia pada saat *system* sedang berjalan, program yang mulai dan berhenti bisa menyimpan datanya dalam registry.

### 1.1. Macam-macam registry Windows

#### 1.1.1 Registry dalam Windows 16-bit

*Registry* dalam sistem Windows 16-bit dimulai pada Windows 3.x yang mana berguna hanya untuk menyimpan asosiasi ekstensi berkas dengan aplikasinya, serta asosiasi objek OLE di dalam dokumen dengan aplikasinya. Implementasi registry dalm windows 16-bit ini masih tergolong yang sangat sederhana.

#### 1.1.2 Registry dalam Windows 9x

Struktur *registry* pada windows 9x hampir sama dengan struktur *registry* dalam Windows NT, tapi tidak kompatibel secara fisik. Dalam sistem operasi windows 9x ini terdapat sebuah anak pohon tambahan, yakni HKEY_DYN_DATA yang digunakan untuk mengukur performa serta melakukan konfigurasi perangkat keras Plug and Play. Windows 9x menyimpan registry di dalam dua berkas yaitu %WINDIR%\system.dat dan %WINDIR%\user.dat. System.dat mengandung informasi mengenai sebuah komputer tertentu, sedangkan user.dat mengandung informasi mengenai user dari komputer tersebut. Contoh windows 9x yaitu Windows 95, Windows 98, dan Windows Millennium Edition.

#### 1.1.3 Registry dalam Windows NT

*Registry* dalam Windows NT sama dengan yang diterapkan pada Windows 2000, Windows XP dan Windows Server 2003 terbagi ke dalam lima buah anak pohon (*subtree*), yang setiap pohon tersebut mengandung kumpulan kunci (*key*) dan anak kunci (*subkey*).

.

## 2. ISI dan PEMBAHSAN

Registry bertugas untuk mengatur semua lalu-lintas yang berada dikomputer, setiap aplikasi yang masuk dan yang keluar(berhenti) akan di atur oleh registry. Selain tiu juga registry bertugas untuk mengatur pemakaian setiap hardware yang telah terdaftara oleh aplikasi-aplikasi yang membutuhkannya. Semuanya tersebut diatur oleh registry karena sudah terlebih dahulu terdaftar di dalamnya.
Struktur dari registry ini berbentuk pohon(tree) seperti halnya windows explorer yang sering kita pakai untuk menelusuri isi dari hardisk. Induk atau root dari registry ini adalah My Computer. Dalam operating sistem seperti windows XP yang sering dipakai oleh masyarakat pada umumnya My computer atau root dari registry ini memiliki 5 buah subpohon (subtree), yaitu :

HKEY_CLASSES_ROOT

HKEY_CURRENT_USER

HKEY_LOCAL_MACHINE

HKEY_USER

HKEY _CURRENT_CONFIG

Setiap subpohon atau upapohon memiliki fungsinya masing-masing. :

- **HKEY_CLASSES_ROOT**
  Sering disingkat **HKCR**, merupakan tempat penyimpananuntuk konfigurasi asosiasi/pemetaan ekstensi sebuah berkas atau objek *Object Linking and Embedding* (OLE) dengan aplikasi yang dapat menanganinya. Sebagai contoh, berkas berekstensi *.doc yang akan ditangani oleh aplikasi microsoft word *.avi yang akan ditangani oleh aplikasi-aplikasi multimedia seperti windows

media classic, media player winnamp dan lainnya.

- **HKEY_CURRENT_USER**
  Nama lainnyaadalah **HKCU**, merupakan sebuah tempat penyimpanan untuk konfigurasi yang dimiliki oleh pengguna yang sedang melakukan *logon*, upa pohon ini menyimpan informasi mengenai konfigurasi preferensi pengguna (konfigurasi *desktop*, warna, dan konfigurasi lainnya yang setiap pengguna dapat melakukan kustomisasi terhadapnya).

- **HKEY_LOCAL_MACHINE**
  Nama lainnya **HKLM**, merupakan sebuah tempat penyimpanan untuk konfigurasi sistem yang bersangkutan, yang terdiri atas perangkat keras dan perangkat lunak. Semua yang terdapat di dalam anak pohon ini diaplikasikan kepada semua pengguna

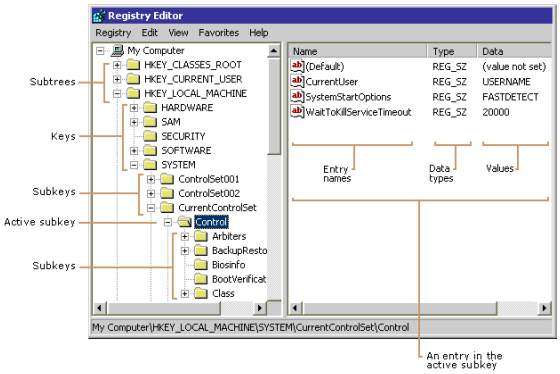
- **HKEY_USER**
  Nama lainnya **HKU**, merupakan tempat penyimpanan untuk konfigurasi setiap pengguna yang terdaftar di dalam komputer yang bersangkutan. Setiap anak kunci dari anak pohon ini diidentifikasikan dengan menggunakan nomor *Security Identifier* (SID) yang dimiliki oleh pengguna. Ketika pengguna melakukan logon, SID yang cocok akan dimuat ke dalam anak pohon HKEY_CURRENT_USER. Anak pohon HKEY_USERS mengandung beberapa anak yakni semua profil pengguna yang terdaftar di dalam sistem yang bersangkutan dan basis data registrasi objek OLE. Selain itu, anak pohon ini juga mengandung HKEY_USERS\.DEFAULT, yang dihubungkan dengan profil milik akun SYSTEM, yang merupakan profil yang digunakan oleh salah satu komponen Windows, WINLOGON.EXE, untuk menyimpan semua konfigurasi seperti halnya HKEY_CURRENT_USER, yakni bagaimana tampilan desktop, bagaimana konfigurasi perangkat keras dan lain-lain. Pengaturan yang diberlakukan terhadap HKU\.DEFAULT ini dapat menjadikan konfigurasi desktop dan lain-lain pada saat proses logon Windows akan berubah dari pengaturan *default*-nya.
  Ketika seorang pengguna masuk log ke sebuah sistem untuk pertama kalinya, sementara akun miliknya tidak berupa *roaming profile* (yakni, sebuah profil pengguna yang disimpan di dalam tempat tersentralisasi di dalam *domain controller*), maka Windows akan membuatkan sebuah profil yang baru untuknya, yang dibuat berbasiskan pengaturan yang terdapat di dalam C:\Documents and Settings\Default User.

- **HKEY_CURRENT_CONFIG**
  Dikanal juga sebagai **HKCC**, merupakan tempat penyimpanan untuk konfigurasi perangkat keras dan sistem operasi yang sedang digunakan saat itu, yang diperoleh pada saat proses booting dilakukan. Informasi yang disimpan di sini bersifat volatil dan tidak disimpan secara permanen ke dalam berkas penampung *registry*, tapi akan selalu dibuat setiap kali proses *booting* dilakukan. Anak pohon HKEY_CURRENT_CONFIG mengandung data konfigurasi untuk profil perangkat keras (*hardware profile*) yang sedang digunakan oleh Windows. HKCC tidak mengandung data apapun, karena memang anak pohon ini merupakan sebuah symbolic link terhadap HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Hardware Profiles\Current. Dengan demikian, dengan mengubah kunci tersebut atau mengubah HKCC, akan menghasilkan sesuatu yang sama.Penggunaan profil perangkat keras mengizinkan administrator untuk mengonfigurasikan beberapa variasi dari pengaturan driver perangkat keras yang digunakan pada saat melakukan booting. Meskipun profil yang digunakan dapat berubah dari satu proses booting ke proses booting lainnya, aplikasi dapat merujuk ke anak pohon ini untuk mencari profil mana yang sedang dimuat oleh Windows. Pengaturan profil perangkat keras dapat dilakukan dengan Control Panel->System->Hardware->Hardware Profiles. Jika ada lebih dari satu profil perangkat keras, maka komponen Windows, yakni NTLDR, akan menanyakan kepada pengguna mengenai profil yang harus dimuat pada saat proses booting dilakukan

Adapun struktur data registry terdiri dari :

- ROOT yang merupakan akar dari pohon struktur registry yaitu My Computer
- Subtree atau subpohon dari ROOT yang terdiri dari 5 HKEY(handle to Key)
- Key, merupakan sub pohon dari Subtree dan berisi kunci dari sub pohon tersebut, contohnya, untuk HKLM atau HKEY_LOCAL_MACHINE key yang termasuk dalam sub pohon ini adalah Hardware, SAM security, software, sistem.
- SubKey, merupakan subpohon dari key berisi informasi dan properties dari key tersebut dan seterusnya.

Seperti yang terlihat pada gambar dibawah ini.
Setiap subpohon (termasuk key dan subkey) memiliki Entry yang menjelaskan properti atau state dari subpohon tersebut.




Dalam registry, elemen entry yang dimasukan ada tiga yaitu entry name, data type dan value.
Sebuah *value* dapat memiliki jenis-jenis data seperti di bawah ini:

- **REG_NONE :** Jenis data registry yang tidak didefinisikan sebelumnya. Jenis data ini secara internal menggunakan tanda pengenal (*identifier*) 0x00.

- **REG_SZ :** Jenis data teks (*string*) dengan panjang yang tetap. Semua sistem operasi 32-bit Windows (Windows NT dan Windows 9x) mendukung jenis data registry ini. Jenis data ini secara internal menggunakan tanda pengenal (*identifier*) 0x01.

- **REG_EXPAND_SZ :** Jenis data teks/*string* yang dapat diekspansi. Windows 9x tidak memiliki jenis data ini. Diperlukan editor *registry* khusus (regedt32.exe) untuk menangani jenis data ini. Jenis data ini secara internal menggunakan tanda pengenal (*identifier*) 0x02.

- **REG_BINARY :** Jenis data biner, yang dapat berarti macam-macam (bisa berupa teks/*string*, atau bilangan). Semua sistem operasi 32-bit Windows (Windows NT dan Windows 9x) mendukung jenis data registry ini. Jenis data ini secara internal menggunakan tanda pengenal (*identifier*) 0x03.

- **REG_DWORD :** Jenis data angka 32-bit. Semua sistem operasi 32-bit Windows (Windows NT dan Windows 9x) mendukung jenis data registry ini. Jenis data ini secara internal menggunakan tanda pengenal (*identifier*) 0x04. Terdapat dua jenis implementasi dari jenis data ini, yakni:
    - **REG_DWORD_LITTLE_ENDIAN**, yang merupakan jenis data REG_DWORD *default* dalam Windows NT yang dijalankan di atas prosesor Intel x86/x64. Jenis data ini berukuran 32-bit yang disusun dengan menggunakan format *little-endian*. Jenis data ini secara internal menggunakan tanda pengenal (*identifier*) 0x05.
    - **REG_DWORD_BIG_ENDIAN**, yang merupakan jenis data REG_DWORD yang berukuran 32-bit yang disusun dengan menggunakan format *big-endian*. Jenis data ini hanya dapat didukung oleh Windows NT yang dijalankan di atas mesin DEC Alpha, MIPS, atau IBM PowerPC, yang memang menggunakan format bilangan *big-endian*. Windows NT 5.x yang hanya dapat berjalan di atas sistem x86 tidak menangani jenis data ini (terdapat limitasi pada mikroprosesor), meskipun Windows NT 5.x mendukungnya. Jenis data ini secara internal menggunakan tanda pengenal (*identifier*) 0x06.

- **REG_MULTI_SZ :** Jenis data teks/*string* yang memiliki banyak baris yang dipisahkan dengan dua buah karakter *null* (0x00). Windows 9x tidak memiliki jenis data ini.Diperlukan editor registry khusus (*regedt32.exe*) untuk menangani jenis data ini. Jenis data ini secara internal menggunakan tanda pengenal (*identifier*) 0x07.

- **REG_LINK :** *Symbolic link* ke sebuah objek Windows NT dalam ruang nama/*namespace* objek Windows NT (yang diatur oleh Object Manager Windows NT). Registry Editor *default* bawaan Windows (*regedit.exe*, *regedt32.exe*, dan utilitas *command-line reg.exe*) tidak dapat menyunting jenis ini. Jenis data ini digunakan secara internal oleh Windows NT saja, dan tidak digunakan oleh aplikasi. Registry dalam Windows 9x tidak memiliki jenis data ini. Jenis data ini secara internal menggunakan tanda pengenal (*identifier*) 0x08.

- **REG_RESOURCE_LIST** (Windows NT) atau **REG_FULL_RESOURCE_DESCRIPTOR :** Jenis data registry yang hanya digunakan untuk menyimpan konfigurasi perangkat keras dan *driver*-nya yang terinstalasi di atas sistem operasi Windows NT. Registry dalam Windows 9x tidak memiliki jenis data ini. Jenis data ini adalah kumpulan larik (array) yang digunakan untuk menyimpan daftar sumber daya (interupsi perangkat keras, *Direct Memory Access* (DMA), *I/O range* dan *memory range*) yang digunakan oleh

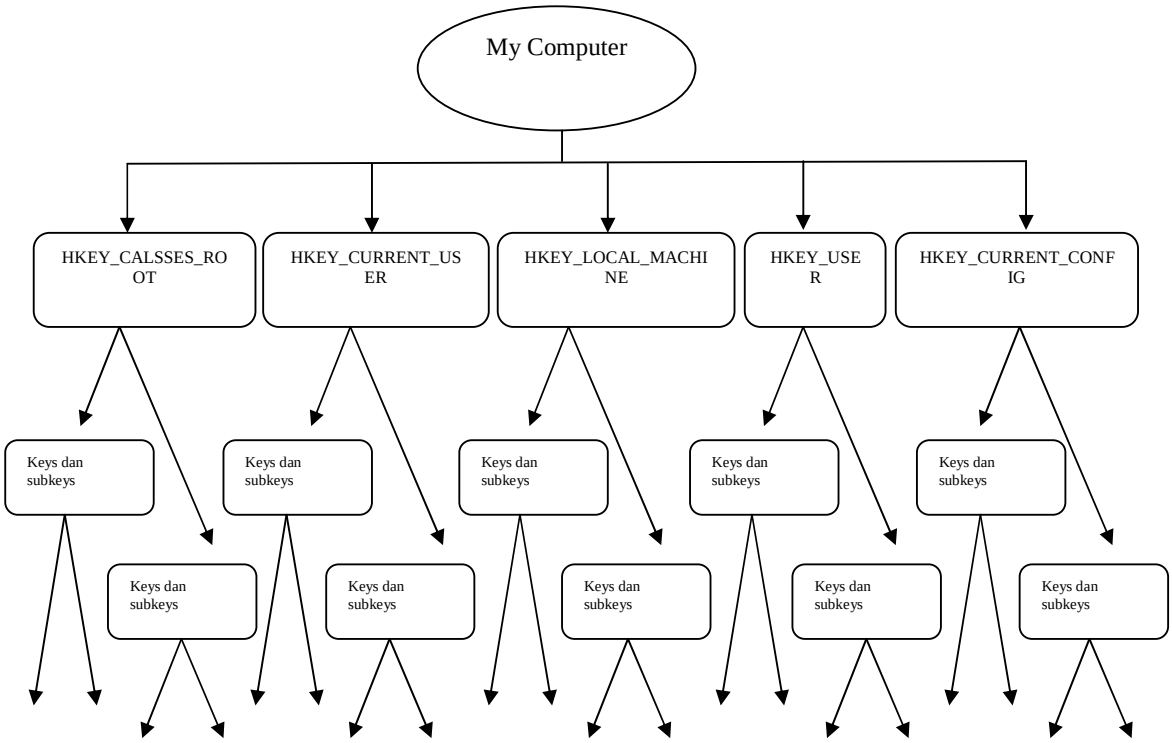
komponen perangkat keras atau *driver*. Dibutuhkan registry editor khusus (*regedt32.exe*) untuk menyunting *value* dengan jenis data ini. Jenis data ini secara internal menggunakan tanda pengenal (*identifier*) 0x09.

- **REG_QWOR :** Jenis data angka yang memiliki panjang 64-bit. Jenis data ini hanya terdapat di dalam sistem prosesor 64-bit saja, semacam DEC Alpha, IA-64, atau x64. Jenis data ini secara internal menggunakan tanda pengenal (*identifier*) 0x12. Sama seperti halnya REG_DWORD, REG_QWORD juga terdapat dua jenis implementasi, yakni *little-endian* (**REG_QWORD_LITTLE_ENDIAN**, dengan identifier 0x13) dan *big-endian* (**REG_QWORD_BIG_ENDIAN**, dengan *identifier* 0x14), meskipun secara *default* format yang digunakan adalah **REG_QWORD_LITTLE_ENDIAN**. Diperlukan editor khusus untuk menyunting jenis data ini.

Meng-*entry* sebuah value bergantung pada tipe data yang kita buat, value dari entry adalah **logika** yang kita masukan untuk menjalankan key tersebut.
Misalkan jika ingin mengunci taskbar maka pada *HKEY_CURRENT_USER/Software/Microsoft/Windows/CurrentVersion/Explorer/Advanced*
Klik ganda pada TaskBarSizeMove dan masukkan angka 0 pada Value Data yang berarti tidak.
Registry windows adalah **himpunan** dari Key-key yang sudah mendapat yang mempunyai fungsi tertentu.

Struktur registry windows mengambil bentuk struktur pohon seperti yang telah dijelaskan sebelumnya, degan my computer sebagai induk atau root dari pohon struktur registry windows tersebut. Untuk lebih jelasnya lihat gambar dibawah.

Dengan menggunakan struktur pohon, dapat terlihat penempatan strukturnya sehingga dapat denga mudah dipahami posisi dan fungsi dari masing-masing key-nya. Misalnya untuk HKEY_LOCAL_MACHINE mempunyai subkey-subkey yang kebanyakan berhubungan dengan hardware. Dengan struktur pohon ini juga konfigurasi yang satu dengan yang lain bisa dipisahkan dalam Registry seperti memisahkan konfigurasi mesin dari konfigurasi pengguna. Ketika seorang pengguna masuk log ke dalam sebuah komputer berbasis Windows NT/2000/XP/Server 2003, pengaturan *registry* yang dimiliki oleh pengguna yang bersangkutan akan dimuat secara terpisah dari konfigurasi sistem operasi yang utama. Hal ini mengizinkan program-program untuk lebih mudah dikonfigurasi untuk setiap orang pengguna (setiap pengguna berhak memiliki preferensi masing-masing), mengingat mereka hanya bekerja di dalam anak pohon "Current User" saja. Sementara itu, jika dibandingkan dengan konfigurasi yang lama, berkas .INI cenderung untuk menulis konfigurasi dan pengaturan setiap program oleh setiap pengguna di dalam satu tempat saja, yakni berkas INI yang bersangkutan.



## 3. KESIMPULAN

Registry adalah jantung dari windows yang berisi hal-hal yang vital yang apabila salah didalam pengubahan maka akan berakibat pada kerusakan sistem.

Struktur dari registry windows mengambil bentuk pohon dengan my computer sebagai rootnya yang kemudian terdapat subpohon-subpohon yang menjadi tonggak sistem tersebut. Setiap subpohon terdapat key-key dan subkey yang mengatur prilaku setiap subpohon tersebut. Setiab key atau subkey bisa dimasukan entry tertentu dengan berbagai tipe data tertentu. Setiap tipedata tertentu memiliki masukan logika yang berbeda bergantung pada entry apa yang dimasukan, seperti untuk quick boot yang entrynya berupa DWORD maka dimasukan angka 1 untuk menyatakan *enable* dan 0 untuk menyatakan *disable*, sedangkan misalnya untuk masukan WaitToKillTimeOut yang bertipe string, masukannya adalah berupa angka yang nantinya registry akan mengintrepetasikan sebagai waktu timeout-nya.

Dengan pendekatan struktur pohon setiap konfigurasi-konfigurasi dalam registry bisa pilah-pilah sehingga memudahkan untuk pengaturan dan meningkatkan performa.

## DAFTAR REFERENSI


[1] http://id.wikipedia.org/wiki/Windows_Registry 5 Januari 2009.

[2] http://www.davescomputertips.com/images/newsletter/2007/071115/an_introduction_to_the_windows_registry.pdf. 5 Januari 2009

[3] http://www.forensicfocus.com/downloads/windows-**registry**-**quick**-reference.pdf 5 Januari 2009