

Windows Registry Tutorial

by WinGuides.com

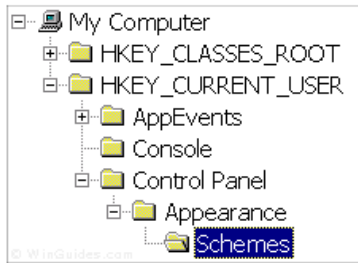
Sistem Kayıt Defteri (Registry) Nedir?

Sistem kayıt defteri Windows 95, 98, Me, Nt/2000, XP gibi 32 bitlik Microsoft Windows versiyonlarının ayarlarının ve seçeneklerinin depolandığı veritabanıdır. Bu veri tabanı tüm donanım, yazılım, kullanıcılar ve PC ilgili bilgileri içerir. Kullanıcı Denetim masasını kullanarak ayarları değiştirdiğinde veya dosya tipleri, sistem politikalarını değiştirdiğinde veya yeni yazılım yüklediğinde sistem kayıt dosyasına gerekli bilgiler kaydedilir.

Sistem kayıt dosyası bilgileri saklamak için sistemdeki USER.DAT ve SYSTEM.DAT dosyalarını kullanır.

Sistem Kayıt Defterinin Yapısı

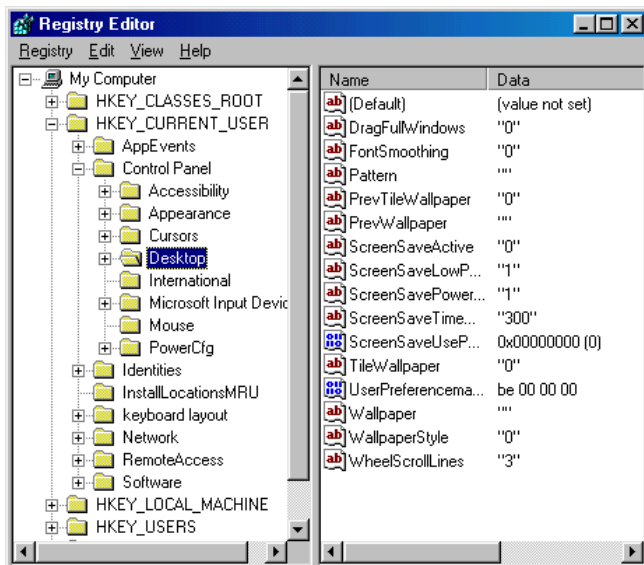
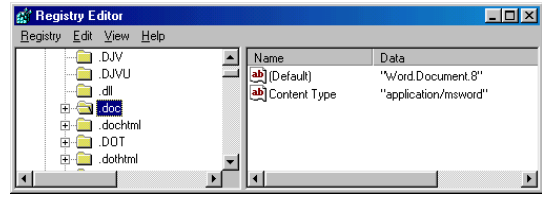
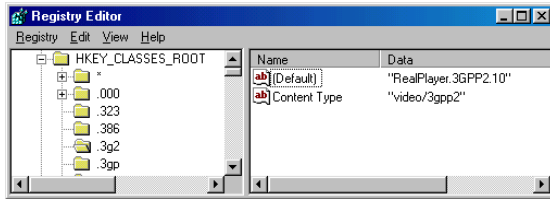
Sistem kayıt defterinin hiyarsşik bir yapısı vardır. Görünüşü hard diskteki dizin yapısına benzer.



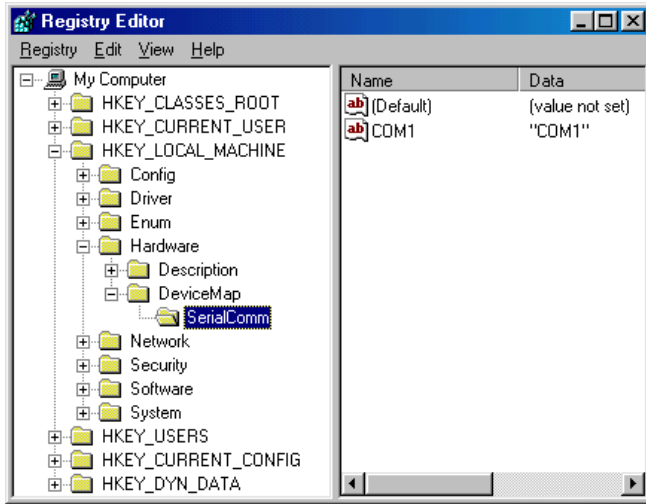
Her bir ana dal (Sistem kayıt defterinde bir klasör olarak gösterilmiştir **Hive (arı kovanı)** olarak adlandırılır, ve hive ler anahtarları (**Keys**) içerirler. Her bir anahtar başka anahtarları içerir. Each key can contain other keys (bazen alt-anahtarlar (**sub-keys**) olarak adlandırılır). Gerçek bilgileri içeren değerler sistem kayıt defterinde (Registry) tutulur. Üç tip değer söz konusudur. *String*, *Binary*, and *DWORD*

Sistem kayıt defterinde özel bilgilerin depolandığı altı ana dal söz konusudur:

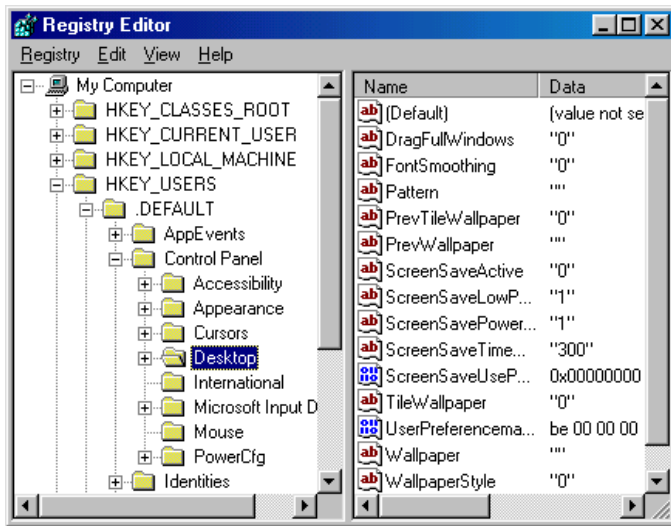
- **HKEY_CLASSES_ROOT** – Bu dal dosyalarla ilgili bilgileri, sürükle bırak olaylarını OLE bilgilerini, windows kısayollarını ve windows kullanıcı arayüzü ile ilgili çekirdek bilgileri içerir.



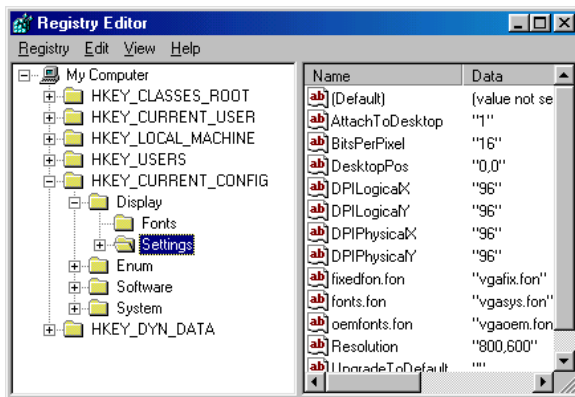
- **HKEY_CURRENT_USER** – Bu dal PC yi logon olmuş kullanıcılara ayrılmıştır ve logon adları, masaüstü ayarları ve başlat menüsü ayarları gibi bilgileri içerir.



- **HKEY_LOCAL_MACHINE** – Bu dal donanım, yazılım ve PC ile gelen seçenekleri içerir. Bilgisayara logon olan kullanıcılar bu bilgileri kullanırlar.



- **HKEY_USERS** – Bu dal bilgisayardaki herhangi bir kullanıcının özel ayarlarını bulundurur. Her bir kullanıcı sub-key içerisinde özel ID ile gösterilir.



- **HKEY_CURRENT_CONFIG** – Bu dal HKEY_LOCAL_MACHINE kısmı ile ilgili olup çalışan donanım konfigürasyonlarını bulundurur.

- **HKEY_DYN_DATA** – Bu dal HKEY_LOCAL_MACHINE dalının bir kısmı ile ilgilidir ve windowsun Tak-Çalıştırını kullanır. Bu kısım dinamiktir. Ve sürücüler eklendikçe ve uzaklaştırıldıkça değişir.

Herbir sistem kayıt değeri beş ana veri tipinden biri şeklinde depolanır.

Name	Data
(Default)	(value not set)
Linked	0x00000001 (1)

New	Key
	String Value
	Binary Value
	DWORD Value

- **REG_BINARY** – Bu tip depolamalar ham binary veriler şeklinde saklanır. Pek çok donanım bilgisi binary veri olarak depolanır ve hekza desimal formatta görülebilir.
- **REG_DWORD** – Bu tip veriler dört byte lık bir sayı gösterir. disable için "0" ve enable "1" gibi basit boolean değerler kullanılır kullanılır. Ayrıca cihaz sürücüleri ve servisler için pek çok parametre bu

tipindedir.

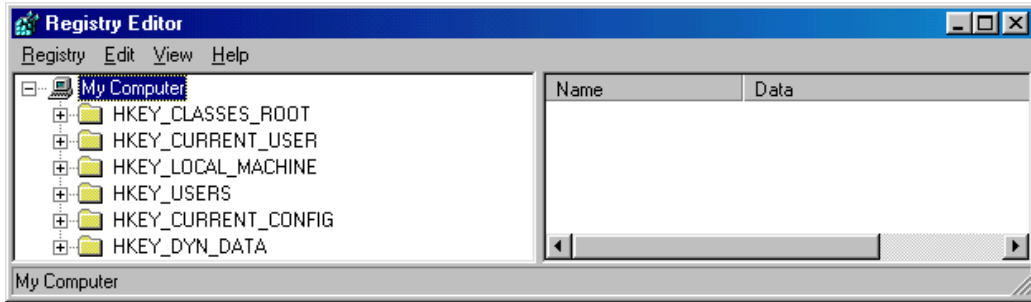
- **REG_EXPAND_SZ** – Bu tip genişleyebilir veri stringlerini içerir. bir uygulama tarafından çağrıldığında değişken ile yer değiştirir. Örneğin; "%SystemRoot%" string değeri Windows NT sistem dosyalarını içeren dizinin gerçek yeriyle yer değiştirebilir.
- **REG_MULTI_SZ** – Bu tip her bir girdinin bir boşluk karakteriyle ayrıldığı liste veya çoklu değerleri içeren verileri kullanılır.
- **REG_SZ** – Bu tip standart bir dizidir. Okunabilir text değerlerdir.

Diğer veri tipleri aşağıda verilmiştir.

- **REG_DWORD_LITTLE_ENDIAN** - little-endian biçiminde 32-bitlik bir sayı
- **REG_DWORD_BIG_ENDIAN** - big-endian biçiminde 32-bitlik bir sayı.
- **REG_LINK** - Unicode sembolik bir link. Uygulamalar bu tipi kullanmaz.
- **REG_NONE** – Belirlenmemiş veri tipi
- **REG_QWORD** - 64-bitlik bir sayı
- **REG_QWORD_LITTLE_ENDIAN** - little-endian biçiminde 64-bitlik bir sayı
- **REG_RESOURCE_LIST** – Bir cihaz sürücüsü kaynak listesi

Sistem Kayıt Defterinin Yazılması

Sistem kayıt defteri editörü (REGEDIT.EXE) windowsların pekçok versiyonunda mevcuttur (gerçi başlat menüsü üzerinde bulunmaz).Bu programla sistem kayıt defterini görür, araştırır, ve düzenleyebilirsiniz. Editörü açmak için Başlat butonuna tıklayın, Çalıştır'ı seçin ve sonra Aç kutusuna regedit yazıp tamam butonuna basın. Eğer Sistem kayıt defteri kurulu ise ve aşağıdaki görüntü ile karşılaşsınız.



Alternatif bir sistem kayıt defteri düzenleyici (REGEDT32.EXE) Windows NT/2000 da kullanılabilir ve ekstra bazı özellikler bulundurur.