5 WINDOWS REGISTRY

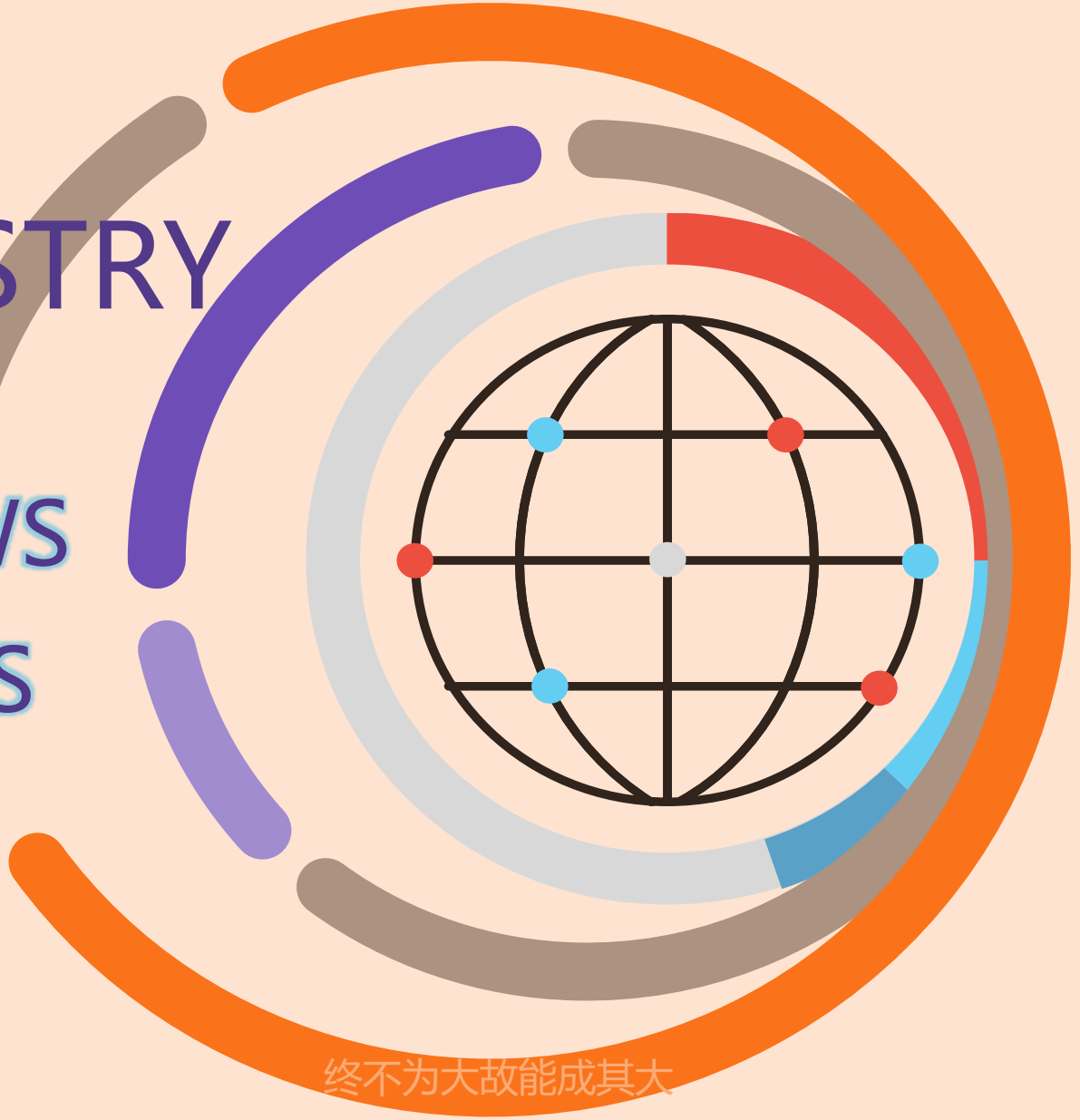
PRINCIPLE OF WINDOWS AND ITS APPLICATIONS

School of CS

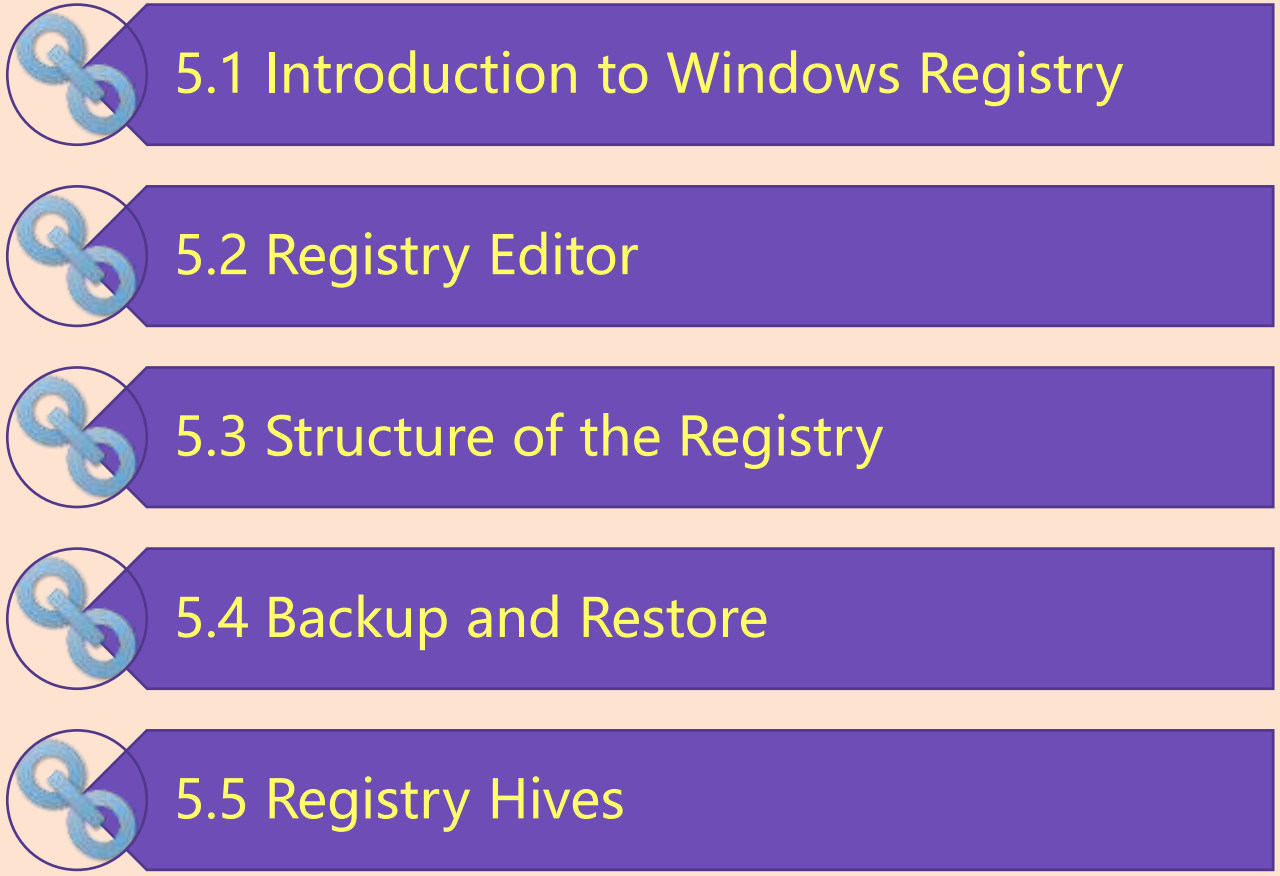
Jicheng Hu

jicheng @ yahoo . com

https://gitee.com/wuhanuniversity/



outlines


5.1 Introduction to Windows Registry
5.2 Registry Editor
5.3 Structure of the Registry
5.4 Backup and Restore
5.5 Registry Hives

概 述

The registry is a system-defined database in which applications and system components store and retrieve configuration data.

- 注册表是 Windows 的一个内部数据库，一个巨大的树状分层数据库。
- 容纳了应用程序和计算机系统的全部配置信息、系统和应用程序的初始化信息、应用程序和文档文件的关联关系、硬件设备的说明、状态和属性以及各种状态信息和数据。
- 注册表中存放着各种参数，直接控制着Windows的启动、硬件驱动程序的装载以及一些Windows应用程序的运行，从而在整个Windows系统中起着核心作用。
- 注册表在Windows 中起到中介的作用，负责系统同软件、硬件、用户之间的沟通

Window 使用注册表初衷：

- 一致性好：所有 Windows 应用程序采用一致的配置，相比 ini 等文本配置文件中自定义的各种配置结构（键值对、XML、Json）在MFC中能进行一致的访问
- 访问速度快：注册表以二进制树形结构存储，访问速度比文本解析快
- 保护版权：商业软件的验证信息隐藏在注册表中，二进制存储方式增加了破解难度，保护了版权

缺陷(Gnome 下 Dconf 有类似问题)：

- 迁移困难，造成对 Windows 上软件的迁移困难，重装系统导致软件也必须重装
- 备份麻烦，Linux 下只需备份 /etc 和 /home 基本解决问题
- 删除软件会有注册表遗留，要使用专门软件清理注册表
- 病毒攻击的对象之一，造成无法修复的损伤（“熊猫烧香”病毒）

Windows 平台下注册表发展趋势：

- 硬件等全局资源的放在注册表中方便管理
- 应用程序对注册表的依赖逐渐减弱，采用领域的社区习惯用法方便开放、迁移
  - 新一代 VS 的配置文件夹 .vs/ 大量使用 .json，方便快速恢复用户工作区现场
  - C# 的 app.config 使用的是 XML

注册表的编辑

- The registry in 64-bit versions of Windows is divided into 32-bit and 64-bit keys
- Many of the 32-bit keys have the same names as their 64-bit counterparts, and vice versa
- The default 64-bit version of Registry Editor (Regedit.exe) that is included with 64-bit versions of Windows displays both 64-bit keys and 32-bit keys
- To open the 32-bit version of Registry Editor, follow these steps:
  - Click Start, and then click Run
  - In the Open box, type %systemroot%\syswow64\regedit, and then click OK.

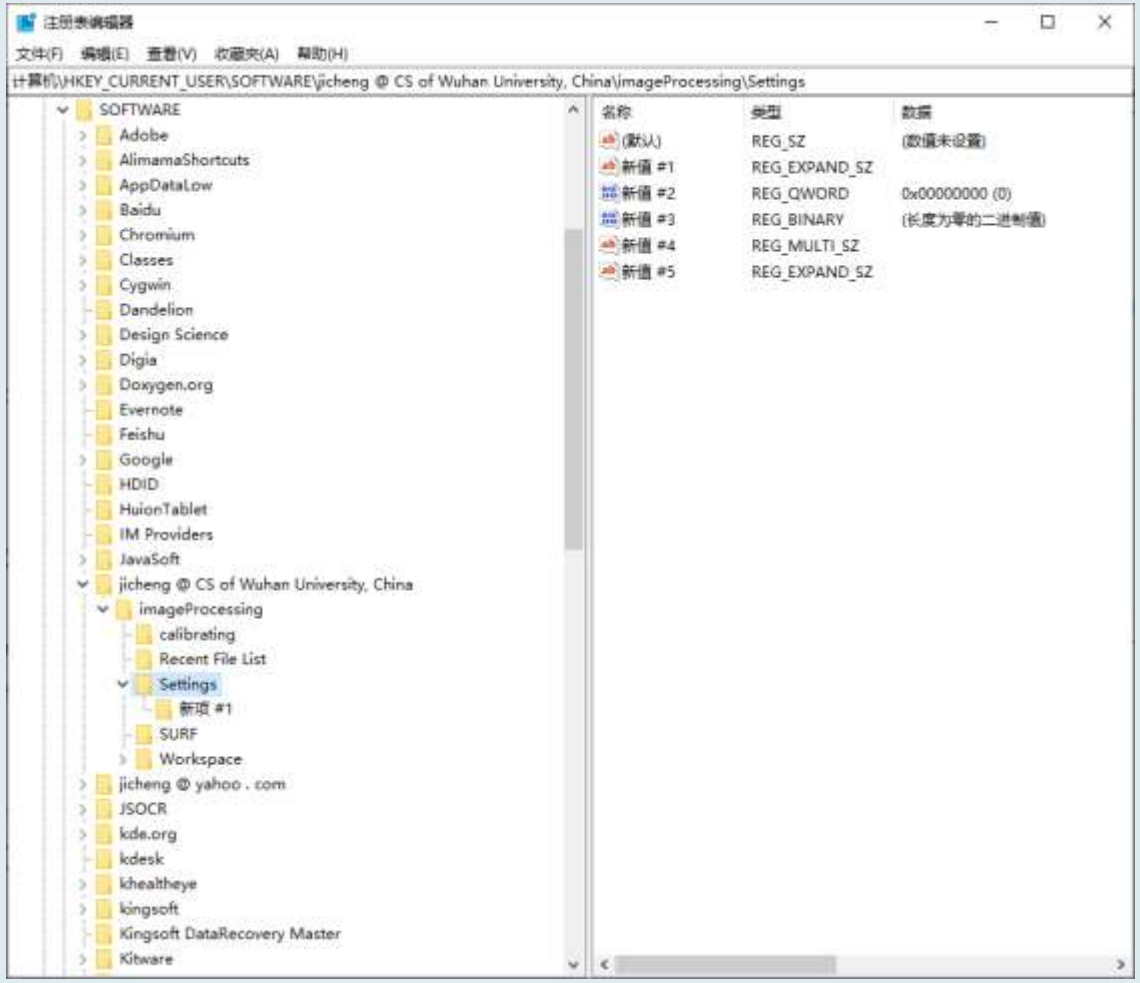
REGEDIT 概述

- 优点
- 不足
  - 安全
  - 特殊数据类型

两个注册表编辑器的比较

- To enable 64-bit/32-bit program interoperability through COM and other mechanisms, WOW64 uses a "Registry Reflector" that mirrors certain registry keys and values between the 64-bit and 32-bit registry views. The reflector is "intelligent", in that is only reflects COM activation data.
- The WOW64 Registry reflector may modify the contents of keys and values during the reflection process to adjust path names, and so on. Because of this, the 32-bit and 64-bit contents may differ. For example, pathnames that contain the system32 registry entry are written as SysWOW64 in the 32-bit section of the registry. The following keys are reflected:
  - HKEY_LOCAL_MACHINE\Software\Classes
  - HKEY_LOCAL_MACHINE\Software\COM3
  - HKEY_LOCAL_MACHINE\Software\Ole
  - HKEY_LOCAL_MACHINE\Software\EventSystem
  - HKEY_LOCAL_MACHINE\Software\RPC

REGEDIT的图形模式



注册表编辑器REGEDT32

- REGEDT32的窗口结构

REGEDT32与REGEDIT窗口的主要差别

- 不是一个单一的窗口，而是五个根键各有一个窗口
- 可以将五个独立窗口中的任意一个最大化，最小化，或重新调整大小，但不能单独关闭其中之一
- 没有“Favorites”菜单
- 在REGEDT32中见不到状态栏
- REGEDT32不支持右击

- REGEDT32用符号显示值类型
  - REG_SZ　　表示“字符串(string)”。
  - REG_BINARY　　表示“二进制(binary)”。
  - REG_DWORD　　表示“DWORD”。
  - REG_MULTI_SZ　表示“多字符串(multi-string)”。
  - REG_EXPAND_SZ　表示“可扩展字符串(expandable string)”，包含一个可扩展变量的字符串。

Registry Element Size Limits

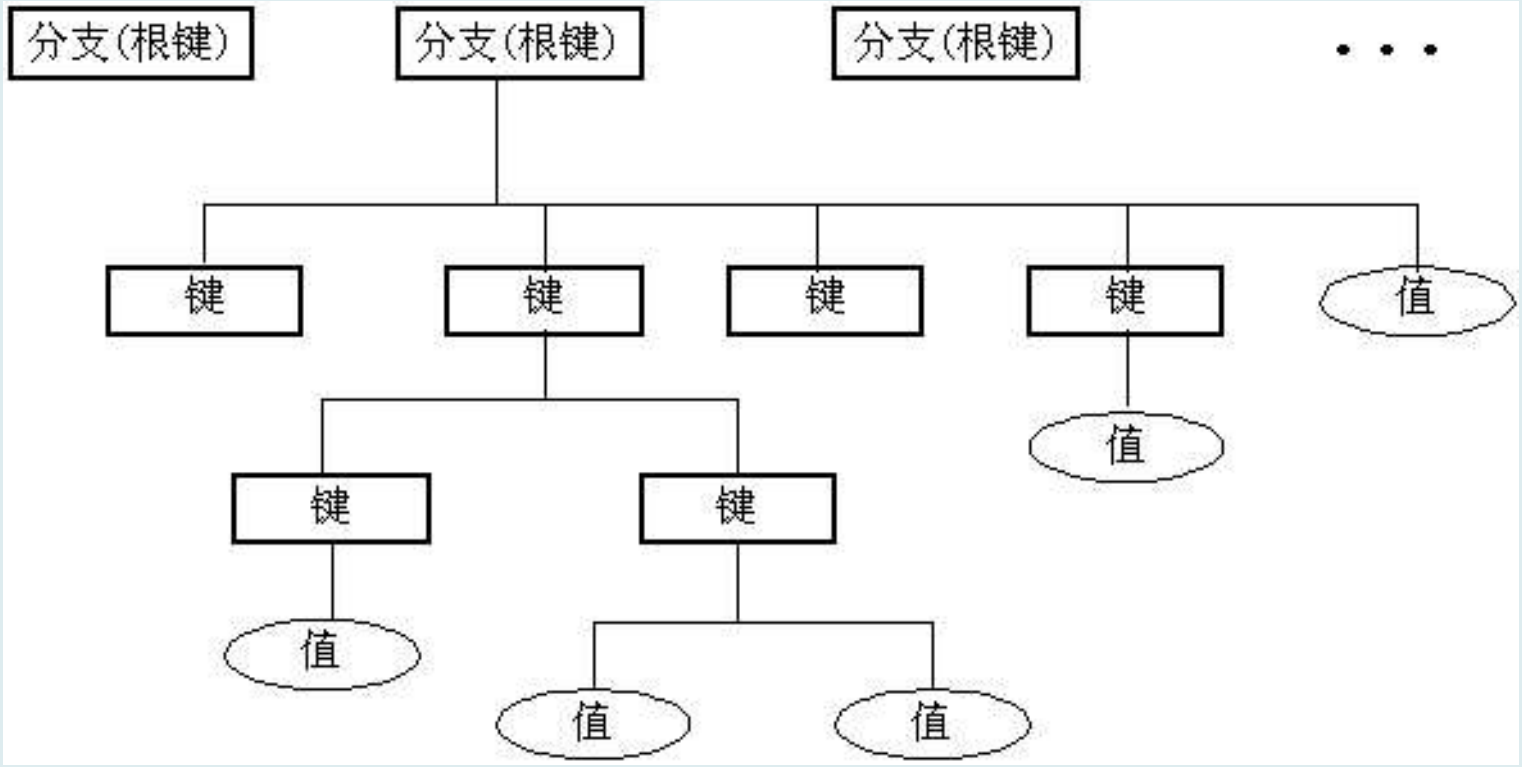
The following table identifies the size limits for the various registry elements.

REGISTRY ELEMENT SIZE LIMITS	
Registry Element	Size Limit
Key name	255 characters. The key name includes the absolute path of the key in the registry, always starting at a base key, for example, HKEY_LOCAL_MACHINE.
Value name	16,383 characters **Windows 2000:** 260 ANSI characters or 16,383 Unicode characters.
Value	Available memory (latest format)1 MB (standard format)
Tree	A registry tree can be 512 levels deep. You can create up to 32 levels at a time through a single registry API call.

Long values (more than 2,048 bytes) should be stored in a file, and the location of the file should be stored in the registry. This helps the registry perform efficiently.

注册表的逻辑结构和内容

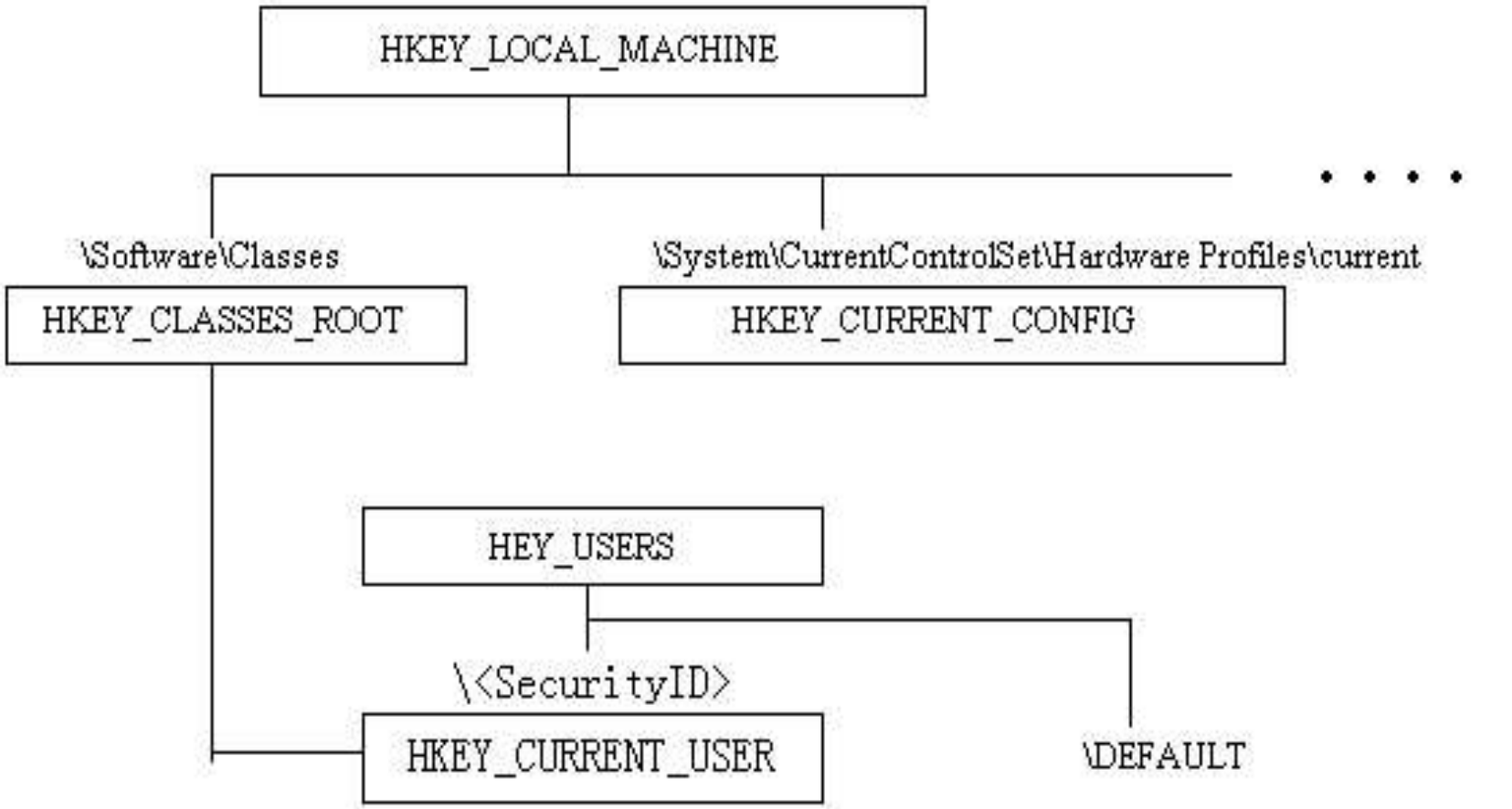
- 注册表的基本组织结构



注册表分支

分支名称	指向	缩写
HKEY_LOCAL_MACHINE		HKLM
HKEY_CURRENT_CONFIG	HKLM\SYSTEM\CurrentControlSet\ Hardware Profiles\Current	HKCC
HKEY_CLASSES_ROOT	HKLM\SOFTWARE\Classes + HKCU\SOFTWARE\Classes	HKCR
HKEY_USER		HKU
HKEY_CURRENT_USER	HKU\<Security ID>	HKCU

注册表分支结构的详细关系图



注册表中的值

- Windows 2000注册表使用三种类型的值：字符串、二进制及DWORD(双字)
- 在注册表编辑器里，值类型是使用前缀REG的“匈牙利语式”符号，例如REG_BINARY

注册表中的值

- 字符串REG_SZ
  - 扩展字符串 REG_EXPAND_SZ，允许用户创建含有一个系统变量的字符串
  - 多重字符串，REG_MULTI_SZ，是字符串类型的另一个变体，是注册表把几个字符串集合成为一个值
- 二进制 REG_BINARY
- DWORD值 REG_DWORD ，是一种特殊的二进制值，即四个字节的二进制值

HKEY_LOCAL_MACHINE

- HKEY_LOCAL_MACHINE(HKLM)
  - 子目录树中的设置内容是关于本地计算机系统的信息，包括硬件和操作系统数据，如总线类型、系统内存、设备驱动程序和启动控制数据。这些信息只与本地的用户有关，而与其他用户无关。
  - 包含五个子项。注意不能使用注册表编辑器修改HKEY_LOCAL_MACHINE子目录树中的SAM子项和SECURITY子项，这些子项对应的是“计算机管理器”等系统功能。

HKEY_LOCAL_MACHINE

- HKEY_LOCAL_MACHINE\HARDWARE
  - 保存了Windows 2000 系统中的所有硬件信息，系统和应用程序都是通过该项的设置与具体的硬件进行沟通。
- HEKY_LOCAL_MACHINE\SOFTWARE
  - 包含系统中软件的设置信息。由于用户安装的软件不同，该项中的设置信息也会不同。
- HEKY_LOCAL_MACHINE\SYSTEM
  - 包含系统启动需要的详细信息，包含设备的驱动程序及其配置信息、控制数据、系统分区及其他驱动器的设置信息，以及系统不能启动时，如何恢复正确配置信息。

HKEY_CURRENT_CONFIG

- HKEY_CURRENT_CONFIG子目录树是用来控制系统硬件配置信息的，它包含系统不同的硬件配置信息之间的差异。如果在系统中设置了多个不同的正确的配置文件，则系统在启动时会让用户选择要使用的配置文件。HKEY_CURRENT_CONFIG控制项代表的就是用户或用户选择的硬件配置文件，但是它只列出用户选择的配置文件与其它配置文件不同的地方。

HKEY_CLASSES_ROOT

- 为了加强对系统数据类型的管理，Windows 在注册表中组织了HKEY_CLASSES_ROOT子目录树，它包含了对数据文件类型的定义；每一种在系统中注册过的文件类型，都会在此建立一个子项。在每一个子项中定义的数据文档的扩展名、扩展名的说明性文字、在文件列表窗口中显示的图标以及与数据文档关联的应用程序和应用程序对数据文档的操作方式。如果用户要动手注册新的数据文档，可以在HKEY_CLASSES_ROOT中创建相应的子项。

HKEY_USERS

- HKEY_USERS子目录树是用来控制用户配置文件的，它包含所有用户的配置文件的内容。每个用户都会在HKEY_USERS项中有一个子项，该子项的内容和HKEY_CURRENT_USER项的内容相似，具体功能也相同，只是使用子项的用户不同。

HKEY_CURRENT_USER

- HKEY_CURRENT_USER子目录树是Windows 注册表最重要的部分之一，它包含Windows 系统、系统的集成部分以及应用软件的配置信息，主要是针对系统的声音、时间、控制面板的功能（如桌面、鼠标、配色方案、屏幕保护程序）、键盘等建立的配置信息以及安装软件时由安装程序建立的项和值

HKEY_CURRENT_USER常用项

- HKEY_CURRENT_USER\AppEvents
- HKEY_CURRENT_USER\Console
- HKEY_CURRENT_USER\Control Panel
- HKEY_CURRENT_USER\Environment
- HKEY_CURRENT_USER\Printers
- HKEY_CURRENT_USER\Keyboard Layout
- HKEY_CURRENT_USER\software

注册表的备份与恢复

- 备份方法
  - 通过REGEDIT菜单工具进行备份。
  - 通过reg.exe工具备份。export
  - 利用磁盘管理工具备份。
- 恢复方法
  - 通过REGEDIT菜单工具进行恢复。
  - 通过reg.exe工具恢复。import
  - 利用磁盘管理工具恢复。

注册表的备份

- Back up the registry manually
  - From the Start menu, type regedit.exe in the search box, and then press Enter. If you are prompted for an administrator password or for confirmation, type the password or provide confirmation.
  - In Registry Editor, locate and click the registry key or subkey that you want to back up.
  - Click File > Export.
  - In the Export Registry File dialog box, select the location to which you want to save the backup copy, and then type a name for the backup file in the File name field.
  - Click Save.
- Create a system restore point
  - From the Start menu, type create a restore point.
  - Select Create a restore point from the search results.
  - Choose Create, and then follow the steps to create a restore point.

注册表的恢复

- Restore a manual back up
  - From the Start menu, type regedit.exe, and then press Enter. If you are prompted for an administrator password or for confirmation, type the password or provide confirmation.
  - In Registry Editor, click File > Import.
  - In the Import Registry File dialog box, select the location to which you saved the backup copy, select the backup file, and then click Open.
- Restore from a restore point
  - From Start, type create a restore point.
  - Select Create a restore point from the search results.
  - Choose System Restore.

注册表文件组成

- 大多数注册表文件都存放在 %SystemRoot%\System32\Config 文件夹
- *.LOG文件，日志文件，保存运行时更新信息。
- Default文件，登录网络前所用缺省用户配置文件。
- Sam (Security Account Manager,安全帐目管理器)
- Security文件，含有与安全有关的内容。
- Software文件，安装软件内容。
- System文件，包含的主要是硬件配置的信息。
- Documents and Settings\UserName\NTUSER.DAT

User Profile Hive

Each time a new user logs on to a computer, a new registry hive is created for that user with a separate file for the user profile. This is called the user profile hive.

- A user's hive contains specific registry information pertaining to the user's application settings, desktop, environment, network connections, and printers
- User profile hives are located under the HKEY_USERS key.

注册表文件组成

The following table lists extensions along with a description of the data in the file

Extension	Description
none	A complete copy of the hive data.
.alt	A backup copy of the critical **HKEY_LOCAL_MACHINE\System** hive. Only the System key has an .alt file.
.log	A transaction log of changes to the keys and value entries in the hive.
.sav	A backup copy of a hive. **Windows Server 2003 and Windows XP/2000:** Copies of the hive files as they looked at the end of the text-mode stage in Setup. Setup has two stages: text mode and graphics mode. The hive is copied to a .sav file after the text-mode stage of setup to protect it from errors that might occur if the graphics-mode stage of setup fails. If setup fails during the graphics-mode stage, only the graphics-mode stage is repeated when the computer is restarted; the .sav file is used to restore the hive data.

注册表文件组成

The following table lists the standard hives and their supporting files

Registry hive	Supporting files
HKEY_CURRENT_CONFIG	System, System.alt, System.log, System.sav
HKEY_CURRENT_USER	Ntuser.dat, Ntuser.dat.log
HKEY_LOCAL_MACHINE\SAM	Sam, Sam.log, Sam.sav
HKEY_LOCAL_MACHINE\Security	Security, Security.log, Security.sav
HKEY_LOCAL_MACHINE\Software	Software, Software.log, Software.sav
HKEY_LOCAL_MACHINE\System	System, System.alt, System.log, System.sav
HKEY_USERS\.DEFAULT	Default, Default.log, Default.sav

上机练习作业

- 使用windows API实现对注册表的操作
  - 创建键与子健
  - 删除键
  - 修改键值
  - 读取键值