Root Keys

Root Key	Description

\HKEY_CLASSES_ROOT (HKCR)	Stores file association and Component Object Model (COM) object registration information.
	
	Component Object Model (COM) is a software architecture developed by Microsoft to build component-based applications. COM objects are discrete components, each with a unique identity, which exposes interfaces that allow applications and other components to access their features. COM objects are more versatile than WIN32 DLLs because they are completely language-independent, have built-in interprocess communications capabilities, and easily fit into an object-oriented program design.
	COM was released in 1993 with OLE, largely to replace the interprocess communications mechanism "DDE" used by the initial release of OLE.
	
	ActiveX is based on COM.
	
	Consists of three types of information:
	• File extension associations
	  ○ A key exists for every registered filename extension
	• COM class registration
	• Virtualized registry root for User Account Control (UAC)
	
	Data under HKCR comes from two sources:
	• Per-user class registration in HKCU\Software\Classes
	  ○ (XP/W2K3) Mapped to \Documents and Settings\<username>\Local Settings\Application Data\Microsoft\Windows\UsrClass.dat
	  ○ (Vista/W2K8) Mapped to \Users\<username>\AppData\Local\Microsoft\Windows\Usrclass.dat.
	• System-wide class registration data in HKLM\Software\Classes

\HKEY_CURRENT_USER (HKCU)	Contains data regarding the preferences and software configuration of the locally logged-on user. It is a pointer to the currently logged-on user's profile. • (XP/W2K3) User's profile located at \Documents and Settings\<username>\ntuser.dat. • (Vista/W2K8) User's profile located at \Users\<username>\ntuser.dat.

\HKEY_LOCAL_MACHINE (HKLM)	The root key that contains all system-wide configuration subkeys.
	• HKLM\BCD (Vista +)
	• HKLM\COMPONENTS (Vista +)
	• HKLM\HARDWARE
	  ○ Hardware configuration data, resource usage
	  ○ Volatile – not saved across boots
	• HKLM\SAM
	  ○ Account and groups database replicated on domain controllers
	• HKLM\SECURITY
	  ○ System-wide security policies on domain controllers
	• HKLM\SOFTWARE
	  ○ Per-machine software data not critical for booting
	• HKLM\SYSTEM
	  ○ Controls booting and running the system

\HKEY_USERS (HKU)	• Contains a subkey for each loaded user profile and user class registration database on the system. • Contains a subkey named HKU\.DEFAULT that is linked to the profile for the system account (used by processes running under the local system's system account). • Also used as a basis for creating a profile for a user account at the user's first logon. • Location where the system stores profiles is defined in the registry value HKLM\Software\Microsoft\Windows. NT\CurrentVersion\profileList\ProfilesDirectory.
\HKEY_CURRENT_CONFIG (HKCC)	• Stores some information about the current hardware profile. • Link to the current hardware profile stored under HKLM\System\CurrentControlSet\Hardware Profiles\Current.
\HKEY_PERFORMANCE_DATA (HKPD)	• A special key that provides access to performance counter information by opening this key and querying the values within it. • The performance information is not actually stored within the registry; the registry functions use this key to locate the information from performance data providers. • Key is only available programmatically through the Windows Registry functions.

HKLM Subkeys

HKLM subkey	Description
HKLM\BCD subkey (Vista\W2K8)	• Contains the Boot Configuration Database - BCD information is loaded as a registry hive during system initialization. • This database replaced the Boot.ini file. • Adds greater flexibility and isolation of per-installation boot configuration data. • BCDEdit is the command-line utility used to modify the BCD. ○ BCD cannot be modified using standard text editors.
HKLM\COMPONENTS subkey (Vista\W2K8)	Contains information pertinent to the Component Based Servicing (CBS) stack (the CBS stack contains various files and resources that are part of a Windows installation image or an active installation). CBS stack: The servicing stack is a set of files and resources that are required to service a Windows image or operating system. It provides various APIs to client installers to service the operating system components (Windows Update, Windows installer, etc.).
HKLM\HARDWARE subkey	• Maintains description of the system's hardware and all hardware device-to-driver mappings. • Device Manager allows you to view the registry hardware information by reading the values out of the HKLM\HARDWARE key.
HKLM\SAM subkey	• Holds the local account and group information, such as user passwords, group definitions, and domain associations. • By default, this key is configured so that even the administrator account doesn't have access.
HKLM\SECURITY subkey	• Stored system-wide security policies and user-rights assignments. • HKLM\SAM is linked to the SAM subkey under HKLM\SECURITY\SAM. • By default, you cannot view the contents of HKLM\SECURITY or HKLM\SAM\SAM as the security settings on those key allow access only by the System account. In order to view these registry keys, you will need to run psexec in the system account (i.e., psexec -s -i -d cmd.exe).
HKLM\SOFTWARE subkey	• Location where Windows stores system-wide configuration information NOT needed to boot the system. • Also, this is the location where third party applications store their system-wide settings.

HKLM\SYSTEM subkey	• Contains the system-wide configuration information needed to boot the system (i.e., which device drivers to load and which services to start). • Windows also maintains a copy of part of this information, called the last known good control set under this key. • Firewall settings within the registry: hklm\system\currentcontrolset\services\sharedaccess\parameters\firewallpolicy • Within FirewallPolicy: Domain Profile Pubic Profile Standard Profile Under each subkey, you will find two subkeys named AuthorizedApplications AND GloballyOpenPorts System-wide rules are located in FirewallRules

Registry Types

These data types can be used to specify the type of a registry value.

Root Key	Description
REG_BINARY	Binary data in any form.
REG_DWORD	32-bit number.
REG_QWORD	64-bit number in little-endian format. In little-endian format, a multibyte value is stored in memory from the lowest byte (the "little end") to the highest byte. For example, the value 0x12345678 is stored as (0x78 0x56 0x34 0x12) in little-endian format.
REG_QWORD_LITTLE_ENDIAN	A 64-bit number in little-endian format. This is equivalent to **REG_QWORD**.
REG_DWORD_BIG_ENDIAN	32-bit number in big-endian format. In big-endian format, a multibyte value is stored in memory from the highest byte (the "big end") to the lowest byte. For example, the value 0x12345678 is stored as (0x12 0x34 0x56 0x78) in big-endian format.
REG_EXPAND_SZ	Null-terminated string that contains unexpanded references to environment variables (for example, "%PATH%"). It will be a Unicode or ANSI string, depending on whether you use the Unicode or ANSI functions.
REG_LINK	Unicode symbolic link.
REG_MULTI_SZ	Array of null-terminated strings that are terminated by two null characters.
REG_NONE	No defined value type.
REG_RESOURCE_LIST	Device-driver resource list.
REG_SZ	Null-terminated string. It will be a Unicode or ANSI string, depending on whether you use the Unicode or ANSI functions.

Managing the Windows Registry

When the need arises to interact with the Windows Registry, this can be completed in one of two ways; graphical interface (regedit) or via command line. If the path/key is already known, it can sometimes be easier to interact with the registry via command line.

Here are a few syntax examples outlining command line use:

Reg query

reg query <KeyName> [{/v <ValueName> | /ve}] [/s] [/se <Separator>] [/f <Data>] [{/k | /d}] [/c] [/e] [/t <Type>] [/z]

Search for the string "C:\Program Files (x86)\Cisco" in "HKEY_LOCAL_MACHINE\Software", no exact match (i.e. partial matches are allowed), case insensitive, search in keys, values and data:

REG Query HKLM\Software /F "C:\Program Files (x86)\Cisco" /S

Reg add

reg add <KeyName> [{/v ValueName | /ve}] [/t DataType] [/s Separator] [/d Data] [/f]

Add the registry key to disable Fast User Switching on the current PC (requires elevation)

REG ADD HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System /v HideFastUserSwitching /t REG_DWORD /d 1

There are two methods to export/save registry data – *export* and *save*
save: Saves a copy of specified subkeys, entries, and values of the registry in a specified file (hiv format).
export: Copies the specified subkeys, entries, and values of the local computer into a file for transfer to other servers (reg format).

Reg save

reg save <KeyName> <FileName> [/y]

Save the hive MyProgram into the current folder as a file named ProgramBkUp.hiv

REG SAVE HKLM\Software\MyCo\MyProgram ProgramBkUp.hiv

Reg export

Reg export KeyName FileName [/y]

Export the contents of all subkeys and values of the key MyProgram to the file ProgramBkUp.reg

reg export HKLM\Software\MyCo\MyProgram ProgramBkUp.reg

Reg import

REG IMPORT FileName.reg

Used to import from the export command

Reg restore

REG RESTORE \\MachineName\[ROOT]\KeyName FileName.hiv

Used to restore from the save command

Recommended Internet Sites

The **Kernel Reference** contains descriptions of kernel programming elements and the **Kernel Functions** table displays the kernel functions with a description of its purpose and whether it can be called in kernel-mode only.

- Kernel Reference https://web.archive.org/save/_embed/https://msdn.microsoft.com/en-us/library/ee482973.aspx
- Kernel Functions https://web.archive.org/web/20160721104739/https://msdn.microsoft.com/en-us/library/ee482951.aspx
- Registry Storage Space https://web.archive.org/web/20160721105013/https://msdn.microsoft.com/en-us/library/windows/desktop/ms724881(v=vs.85).aspx
- Export WinNT Registry Entries
- https://web.archive.org/web/20150215042016/http://support.microsoft.com:80/kb/168589
- Reg save https://web.archive.org/web/20150111070649/https://technet.microsoft.com/en-us/library/cc742108.aspx
- Reg add https://web.archive.org/web/20160721105853/https://technet.microsoft.com/en-us/library/cc742162.aspx
- Reg query https://web.archive.org/web/20160721105928/https://technet.microsoft.com/en-us/library/cc742028.aspx

Please contact the Course Coordinators if you are unable to access any of the Recommended Internet Sites.