The Registry

Mario Tayah and Jim Fawcett

CSE 775 – Distributed Objects

Spring 2007

Definition

- The registry is a database file or presentation that is used by all windows operating systems that followed Win95.
- The registry is used by the Windows OS to store hardware and software configuration information, user preferences and setup information.
- The correct registry is essential for correct windows performance and functioning, this is why the registry is usually attacked by viruses and other malicious software.

Registry vs. File System

- The registry is analogous to a file system.

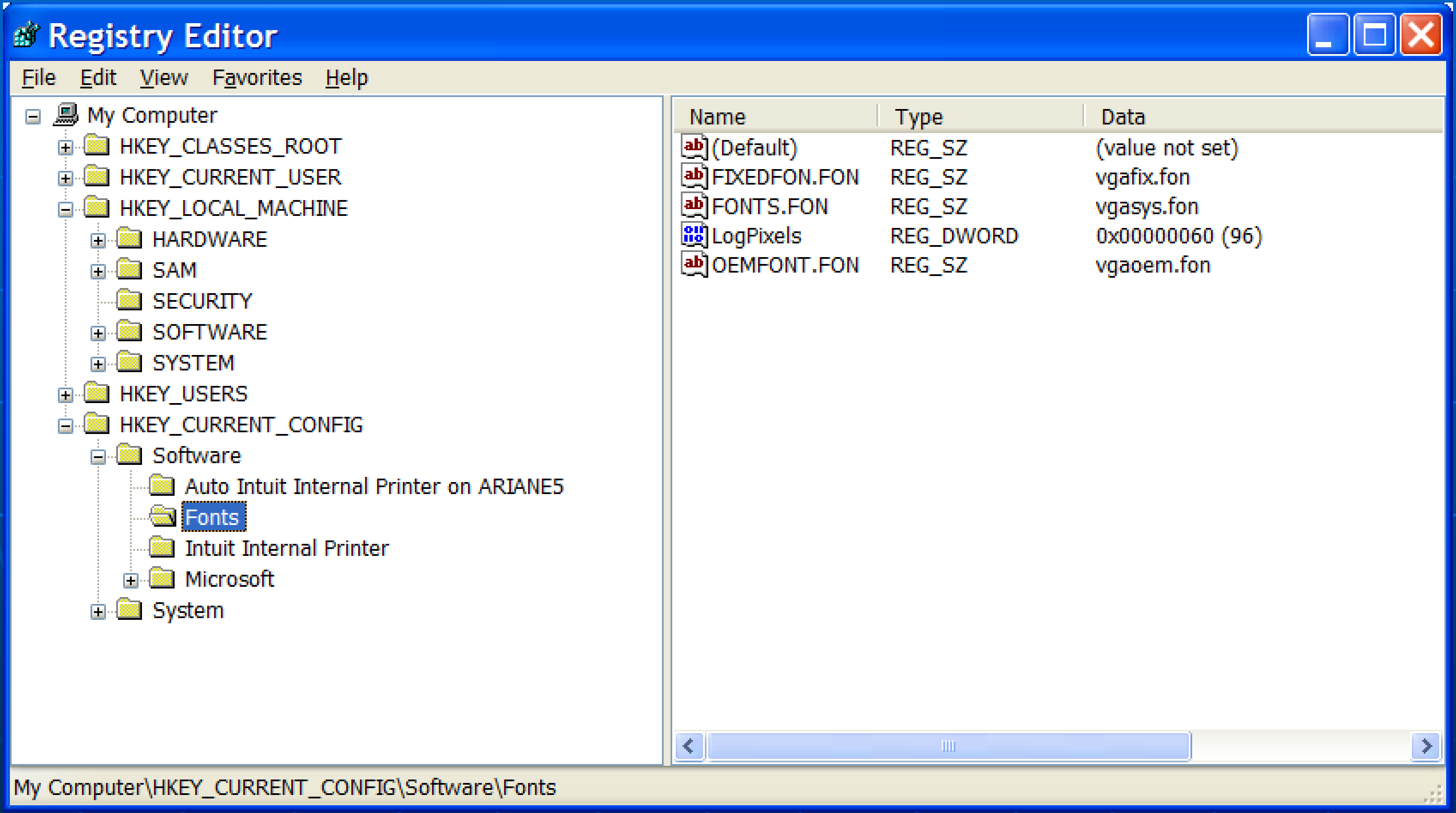
  File system:

  - Folders
  - Files

  Registry:

  - Keys
  - Keys have inside them either other keys or name/value pairs which correspond to object name and content.

Registry Structure



```
My Computer
    HKEY_CLASSES_ROOT
    HKEY_CURRENT_USER
    HKEY_LOCAL_MACHINE
        HARDWARE
        SAM
        SECURITY
        SOFTWARE
        SYSTEM
    HKEY_USERS
    HKEY_CURRENT_CONFIG
        Software
            Auto Intuit Internal Printer on ARIANE5
            Fonts
            Intuit Internal Printer
            Microsoft
        System
```

Name	Type	Data
(Default)	REG_SZ	(value not set)
FIXEDFON.FON	REG_SZ	vgafix.fon
FONTS.FON	REG_SZ	vgasys.fon
LogPixels	REG_DWORD	0x00000060 (96)
OEMFONT.FON	REG_SZ	vgaoem.fon

My Computer\HKEY_CURRENT_CONFIG\Software\Fonts

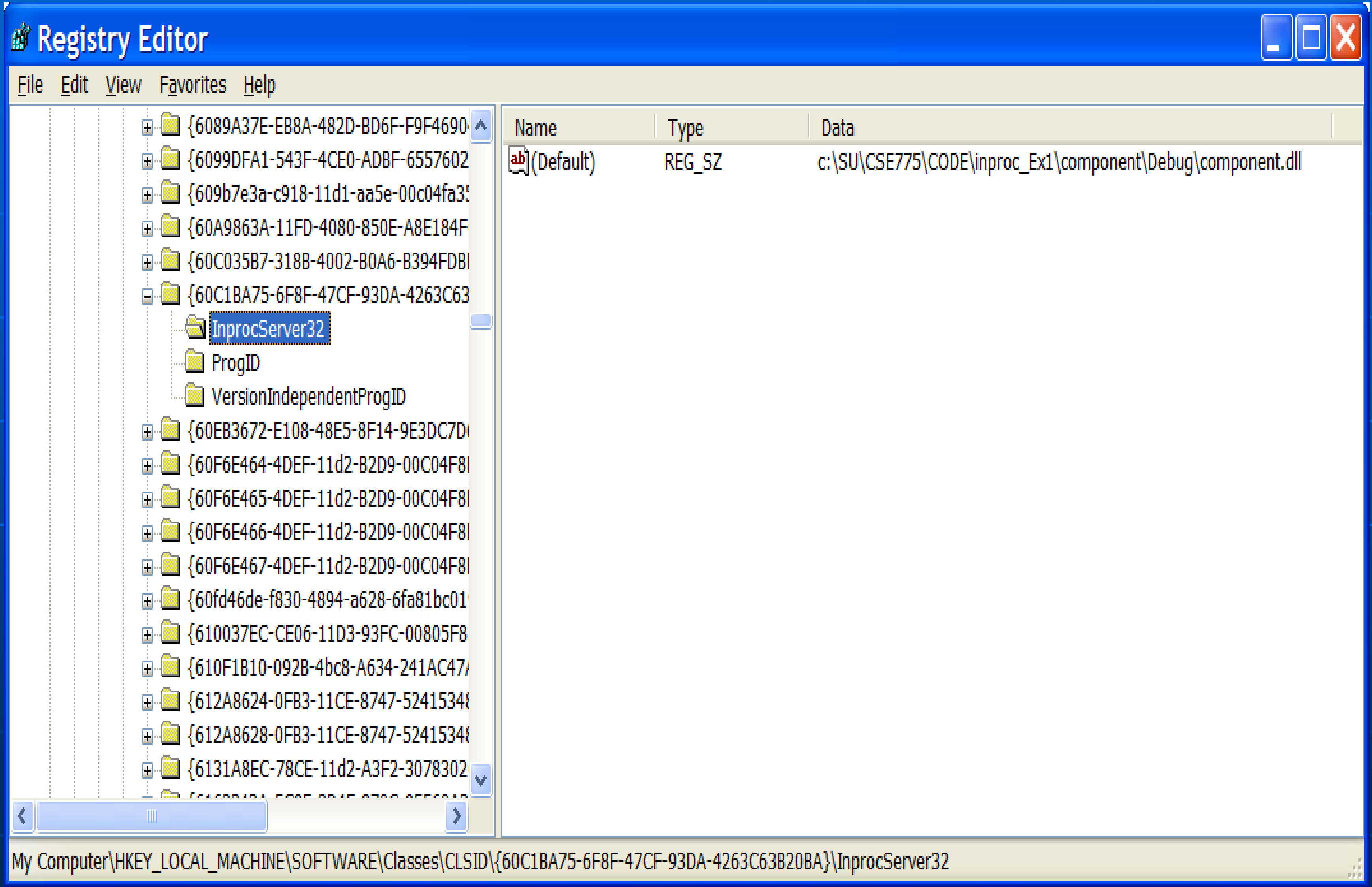
Registry Structure

- Registry has five top level branches or Hives:
  - HKEY_CLASSES_ROOT
    - COM server info, file associations, shortcuts
  - HKEY_CURRENT-USER
    - Logged in user name, desktop, start menu
  - HKEY_LOCAL_MACHINE
    - Hardware, software, preferences for all users
  - HKEY_USERS
    - Individual preferences for each user, represented by Security ID (SID)
  - HKEY_CURRENT_CONFIG
    - Links to part of HKEY_LOCAL_MACHINE for current hardware
  - HKEY_DYN_DATA
    - Links to part of HKEY_LOCAL_MACHINE for PlugAndPlay

Registry Value Types

- REG_BINARY
  - Raw binary data
- REG_DWORD
  - 32 bit integers – often representing bools
- REG_SZ
  - string
- REG_EXPAND_SZ
  - Expandable string
- REG_MULTI_SZ
  - Container for null seperated strings

COM Registry Entry



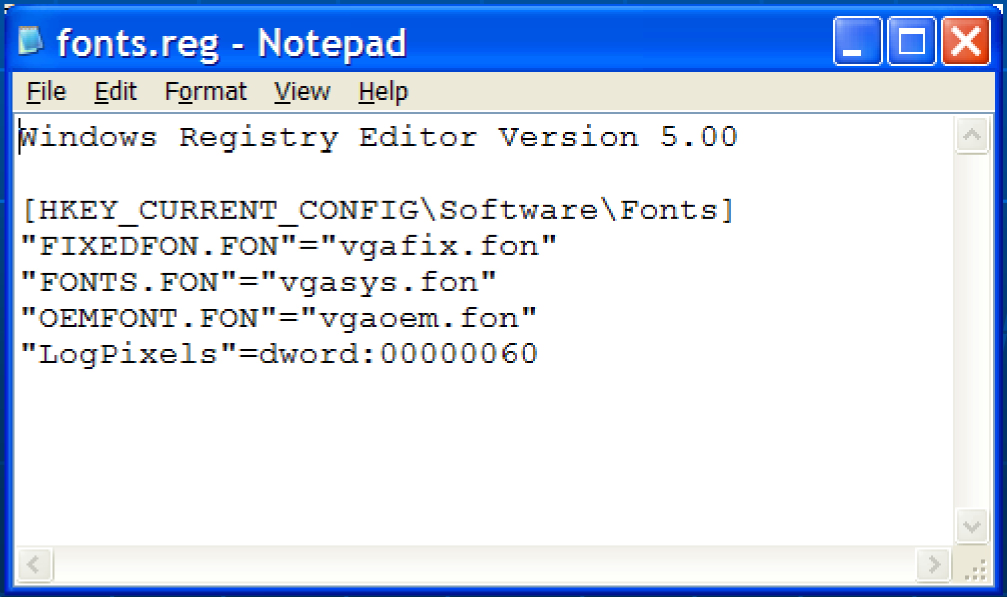
```
{6089A37E-EB8A-482D-BD6F-F9F4690
{6099DFA1-543F-4CE0-ADBF-6557602
{609b7e3a-c918-11d1-aa5e-00c04fa3
{60A9863A-11FD-4080-850E-A8E184F
{60C035B7-318B-4002-B0A6-B394FDB
{60C1BA75-6F8F-47CF-93DA-4263C63
    InprocServer32
    ProgID
    VersionIndependentProgID
{60EB3672-E108-48E5-8F14-9E3DC7D
{60F6E464-4DEF-11d2-B2D9-00C04F8
{60F6E465-4DEF-11d2-B2D9-00C04F8
{60F6E466-4DEF-11d2-B2D9-00C04F8
{60F6E467-4DEF-11d2-B2D9-00C04F8
{60fd46de-f830-4894-a628-6fa81bc01
{610037EC-CE06-11D3-93FC-00805F8
{610F1B10-092B-4bc8-A634-241AC47
{612A8624-0FB3-11CE-8747-5241534
{612A8628-0FB3-11CE-8747-5241534
{6131A8EC-78CE-11d2-A3F2-3078302
```

Name	Type	Data
ab (Default)	REG_SZ	c:\SU\CSE775\CODE\inproc_Ex1\component\Debug\component.dll

My Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{60C1BA75-6F8F-47CF-93DA-4263C63B20BA}\InprocServer32

Exporting and Importing

- In RegEdit select a key
- File Export
- Provide filespec info in resulting save dialog



```
Windows Registry Editor Version 5.00

[HKEY_CURRENT_CONFIG\Software\Fonts]
"FIXEDFON.FON"="vgafix.fon"
"FONTS.FON"="vgasys.fon"
"OEMFONT.FON"="vgaoem.fon"
"LogPixels"=dword:00000060
```

Registry Content

- The registry holds critical information about the system, the users of the system, and installed applications:
  - Operating System version number, build number, and registered user.
  - Informaiton for every properly installed application,
  - Information about the computer’s processor type and system memory.
  - User-specific information (home directory, app. preferences)
  - Security informaiton such as user account names.
  - Installed services
  - Mapping from file names to programs/executables.
  - Mapping network addressees to host machine names.

Registry Programming interface

- The registry programming interface holds a list of functions that can be divided into:
  - Key management (browse, add, remove keys) and includes:
    - RegOpenKeyEx : opens a key and gives you a handle to it.
    - RegEnumKeyEX : provides an enumerator over a key content.
    - CreateKeyEX : creates a new key.
    - RegDeleteKey : deletes a key.
  - Value management (add, remove, edit values of keys):
    - RegEnumValue : Enumerates the values for the specified open registry key.
    - RegSetValueEx : Sets the data for the default or unnamed value of a specified registry key.
    - RegQueryValueEX : Retrieves the type and data for the specified value name associated with an open registry key.
- NOTE: these are the basic and most used functions, you can find the whole interface functions on http://msdn.microsoft.com.

RegOpenKeyEx

- **LONG RegOpenKeyEx(**
  HKEY hKey, LPCTSTR lpSubKey,
  DWORD ulOptions, REGSAM samDesired, PHKEY phkResult).
  - hKey: handle to an open registry key. This handle is returned by the RegCreateKeyEx or RegOpenKeyEx function, or it can be one of the predefined keys.
  - lpSubKey: registry sub key to be opened. Key names are not case sensitive. If this parameter is NULL or a pointer to an empty string, the function will open a new handle to the key identified by the hKey parameter.
  - ulOptions: parameter is reserved and must be zero.
  - samDesired: mask that specifies desired access rights to the key. Fails if the security descriptor of the key does not permit requested access.
  - phkResult: pointer to variable that receives a handle to the opened key. If key is not one of the predefined registry keys, call the RegCloseKey function after you have finished using the handle.

RegEnumKeyEx

- LONG RegEnumKeyEx(HKEY hKey, DWORD dwIndex,   LPTSTR lpName, LPDWORD lpcName, LPDWORD lpReserved,   LPTSTR lpClass, LPDWORD lpcClass, PFILETIME lpftLastWriteTime);
  - HKEY hKey :A handle to an open registry key.
  - DWORD dwIndex: The index of the subkey to retrieve. This parameter should be   zero for the first call to the RegEnumKeyEx function and then incremented for subsequent calls.

    Note :Because subkeys are not ordered, any new subkey will have an arbitrary index. This means that the function may return subkeys in any order.
  - LPTSTR lpName: A pointer to a buffer that receives the name of the subkey, including the terminating null character. The function copies only the name of the subkey, not the full key hierarchy, to the buffer.
  - LPDWORD lpcName: A pointer to a variable that specifies the size of the buffer specified by the lpName parameter, in TCHARs. This size should include the terminating null character. When the function returns, the variable pointed to by lpcName contains the number of characters stored in the buffer. The count returned does not include the terminating null character
  - LPDWORD lpReserved : This parameter is reserved and must be NULL.
  - LPTSTR lpClass: A pointer to a buffer that receives the null-terminated class string of the enumerated subkey.

    NOTE: This parameter can be NULL.
  - LPDWORD lpcClass: A pointer to a variable that specifies the size of the buffer specified by the lpClass parameter, in TCHARs. The size should include the terminating null character. When the function returns, lpcClass contains the number of characters stored in the buffer. The count returned does not include the terminating null character. This parameter can be NULL only if lpClass is NULL.
  - PFILETIME lpftLastWriteTim :A pointer to a variable that receives the time at which the enumerated subkey was last written. This parameter can be NULL

RegCreateKeyEX

- LONG RegCreateKeyEx(HKEY hKey, LPCTSTR lpSubKey, DWORD Reserved, LPTSTR lpClass, DWORD dwOptions, REGSAM samDesired, LPSECURITY_ATTRIBUTES lpSecurityAttributes, PHKEY phkResult, LPDWORD lpdwDisposition);
  - hkey: a handle to a registry key.
  - lpSubKey: The name of a subkey that this function opens or creates. The subkey specified must be a subkey of the key identified by the hKey parameter; it can be up to 32 levels deep in the registry tree.

    Note: this cannot be Null.
  - Reserved : This parameter is reserved and must be zero.
  - lpClass : The class (object type) of this key. This parameter may be ignored and can be NULL. This parameter is used for both local and remote registry keys.
  - dwOptions: this basically indicates wheather this entry is volatile or is stored on file and persists even after the machine is restarted.
  - samDesired :A mask that specifies the access rights for the key.
  - lpSecurityAttributes: A pointer to a SECURITY_ATTRIBUTES structure that determines whether the returned handle can be inherited by child processes. If lpSecurityAttributes is NULL, the handle cannot be inherited.
  - phkResult : A pointer to a variable that receives a handle to the opened or created key. If the key is not one of the predefined registry keys, call the RegCloseKey function after you have finished using the handle.
  - lpdwDisposition: indicats weather this key is already been created or not.

RegDeleteKey

- LONG RegDeleteKey(HKEY hKey, LPCTSTR lpSubKey);
    - Hkey: a handle to an open key in the registry.
    - lpSubKey : The name of the key to be deleted. It must be a subkey of the key that hKey identifies, but it cannot have subkeys.

      NOTE: This parameter cannot be NULL.

      NOTE: Key names are not case sensitive

RegEnumValue

- LONG RegEnumValue(HKEY hKey, DWORD dwIndex, LPTSTR lpValueName, LPDWORD lpcValueName, LPDWORD lpReserved, LPDWORD lpType, LPBYTE lpData, LPDWORD lpcbData);
  - hKey: a handle to an open registry key.
  - dwIndex: the index of the value to be retreived.
  - lpValueName: a buffer that will hold the name of the value.
  - lpcValueName: A pointer to a variable that specifies the size of the buffer pointed to by the lpValueName parameter, in TCHARs.
  - lpReserved: this parameter is reserved and must be zero.
  - lpType: the buffer that will hold the type of the value.
  - lpData: the buffer that will hold the actual value.
  - lpcbData: A pointer to a variable that specifies the size of the buffer pointed to by the lpData parameter, in bytes.

RegSetValueEx

- LONG RegSetValueEx(HKEY hKey, LPCTSTR lpValueName, DWORD Reserved, DWORD dwType, const BYTE* lpData, DWORD cbData);
    - hKey: a registry key handle.
    - lpValueName: The name of the value to be set. If a value with this name is not already present in the key, the function adds it to the key.
    - Reserved: This parameter is reserved and must be zero.
    - dwType: The type of data pointed to by the *lpData* parameter.
    - lpData: The data to be stored.
    - cbData: The size of the information pointed to by the lpData parameter, in bytes. If the data is of type REG_SZ, REG_EXPAND_SZ, or REG_MULTI_SZ, cbData must include the size of the terminating null character or characters.

RegQueryValueEx

- LONG RegQueryValueEx(HKEY hKey, LPCTSTR lpValueName, LPDWORD lpReserved, LPDWORD lpType, LPBYTE lpData, LPDWORD lpcbData);
  - hKey: a handle of a registry key.
  - lpValueName: The name of the registry value.
  - lpReserved: This parameter is reserved and must be NULL.
  - lpType: A pointer to a variable that receives a code indicating the type of data stored in the specified value.
  - lpData: A pointer to a buffer that receives the value's data. This parameter can be NULL if the data is not required.
  - lpcbData: A pointer to a variable that specifies the size of the buffer pointed to by the *lpData* parameter, in bytes. When the function returns, this variable contains the size of the data copied to *lpData*.

Complete Registry interface

Below is a list of all the registry functions:

- RegCloseKey
- RegOpenKey
- RegConnectRegistry
- RegOpenKeyEx
- RegCreateKey
- RegQueryInfoKey
- RegCreateKeyEx
- RegQueryMultipleValues
- RegDeleteKey
- RegQueryValue
- RegDeleteValue
- RegQueryValueEx
- RegEnumKey
- RegReplaceKey
- RegEnumKeyEx
- RegRestoreKey
- RegEnumValue
- RegSaveKey
- RegFlushKey
- RegSetKeySecurity
- RegGetKeySecurity
- RegSetValue
- RegLoadKey
- RegSetValueEx
- RegNotifyChangeKeyValue
- RegUnLoadKey

References

- Windows System Programming, Third Edition, Johnson M. Hart, Addison-Wesley, 2005
- MSDN
- http://docs.rinet.ru/NTServak