Registry Summary Reports

Dustin Hurlbut

For more information contact: info@syntricate.com

NTUSER.DAT RSRs

NTUSER.DAT – Computer Networks.rsr

- Computer Networks documents the registry subkey that tracks network systems the machine has been attached to. It displays data to the user interface in My Network Places, storing the list of other users on the system.

- HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\ComputerDescriptions

NTUSER.DAT – IE E-Mail Account Manager.rsr

- Displays the Internet Account Manager information for e-mail accounts set up locally using Outlook or Outlook Express. It ties into information seen in the PSSP regarding locally stored email passwords in the INETCOMM Server Passwords subkey.

- HKCU\Software\Microsoft\Internet Account Manager\<account name>

NTUSER.DAT – IE Info.rsr

- This RSR displays information regarding the Internet Explorer settings from the Main subkey, URL History Setting showing the number of days the system retains Internet history, and the user's Favorites as seen in the IE Favorites drop down menu which are also stored in the registry.

- HKCU\Software\Microsoft\Internet Explorer\Main

- HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Url History / DaysToKeep

- HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\MenuOrder\Favorites

SYNTRICATE

Registry Summary Reports

Dustin Hurlbut

For more information contact: info@syntricate.com

NTUSER.DAT – Map Network Drive MRU.rsr

- This MRU registry key set displays mapped network drives it has been connected to draw the display of other users on the system from My Network Places.
- HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Map Network Drive MRU

NTUSER.DAT – Media Player MRUs.rsr

- MRU list of last played files through the application Media Player.
- HKCU\Software\Microsoft\Windows\MediaPlayer\Player\RecentFileList

NTUSER.DAT – PSSP Information.rsr

- Protected Storage Information in Windows XP/Windows 2000 systems. Includes the following: Outlook and Outlook Express stored passwords, website form data, stored website logon user names and passwords, and Internet search engine queries.
- HKCU\Software\Microsoft\Windows\Protected Storage System Provider\<sid>\Identification\INETCOMM Server Passwords
- HKCU\Software\Microsoft\Windows\Protected Storage System Provider\<sid>\Internet Explorer\Internet Explorer

NTUSER.DAT – Recent Docs.rsr

- MRU list for recently opened documents by extension.
- HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\ <extension>

SYNTRICATE

Registry Summary Reports

Dustin Hurlbut

For more information contact: info@syntricate.com

NTUSER.DAT – RunMRUs.rsr

- MRU list used to generate the auto complete in the Start > Run drop down menu list.
- HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\RunMRU

NTUSER.DAT – Startup Software by User.rsr

- Standard list of software initiated upon bootup by a specific user.
- HKCU\Software\Microsoft\Windows\CurrentVersion\Run

NTUSER.DAT – Typed URLs.rsr

- MRU list of the last 25 URL addresses typed or copy/pasted into the Internet Explorer browser.
- HKCU\Software\Microsoft\Internet Explorer\TypedURLs

NTUSER.DAT – Vista ComDlg32.rsr

- For Vista systems, this recovers the MRU list of applications where the default Windows Save/Save As dialog box was used.
- HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32

NTUSER.DAT – XP ComDlg32 MRUs.rsr

- For Vista systems, this recovers the MRU list of applications where the default Windows Save/Save As dialog box was used.
- HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32

SYNTRICATE

Registry Summary Reports

Dustin Hurlbut

For more information contact: info@syntricate.com

NTUSER.DAT – WinZip Information.rsr

- This recovers WinZip 11 file list MRU information for Zips and extracted to files.
- HKCU\Software\Nico Mak Computing\WinZip

NTUSER.DAT – XP Local Search Terms.rsr

- This recovers the four varieties of user's local searches initiated with the Start > Search utility in Windows 2000 and Windows XP.
- HKCU\Software\Microsoft\Search Assistant\ACMru\5001 (Local Internet Searches)
- HKCU\Software\Microsoft\Search Assistant\ACMru\5603 (All Files and Folders)
- HKCU\Software\Microsoft\Search Assistant\ACMru\5604 (Pictures Music or Video)
- HKCU\Software\Microsoft\Search Assistant\ACMru\5647 (Computers or People)

SAM File RSRs

SAM – Users.rsr

- List of users with logon credentials for the system.
- HKLM\SAM\SAM\Domains\Account\Users

SYNTRICATE

Registry Summary Reports

Dustin Hurlbut

For more information contact: info@syntricate.com

SAM – Group Names

- Includes Built-n default alias names and custom alias names created by a user. Can be used to fill in missing relative identifiers of users as RIDs are used for groups as well as users.
- HKLM\SAM\Domains\Builtin\Aliases
- HKLM\SAM\Domains\Account\Aliases

SOFTWARE File RSRs

SOFTWARE – Installed Devices.rsr

- In Microsoft Vista, this displays USB drives attached to the system in individual subkeys by their Disk and Vendor name and Drive Identifier and by their volume name in the FriendlyName value associated with each subkey.
- HKLM\SOFTWARE \Microsoft\Windows Portable Devices\Devices\<drive>

SOFTWARE – Installed Software.rsr

- Documents software on the system that uses uninstall programs for removal. Essentially shows a list of installed software.
- HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\<software name>

SOFTWARE – Last Logged On User.rsr

- In Windows Vista, recovers registry entries defining when the last logged on user logged off by user name with a date and time reference as the subkey is updated.
- HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Authentication\LogonUI

SYNTRICATE

Registry Summary Reports

Dustin Hurlbut

For more information contact: info@syntricate.com

SOFTWARE – Printers.rsr

- Displays information regarding printers configured to the system
- HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Print\Printers\<printer name>

SOFTWARE – Profile List.rsr

- This key set lists each of the user file system profiles in either Documents and Settings (XP) or Users (Vista). This keyset is not created until a newly created user logs on for the first time.
- HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfilesList\<user sid>

SOFTWARE – ReadyBoost.rsr (Vista)

- ReadyBoost in Vista allows the user to identify a USB as extra RAM. The ReadyBoost key set defines USB drives that have been attached to the system and identifies them by both their drive identifier and their volume name. Within the subkey that contains this information is potential info about the USB device if it was tested for use as extra memory.
- HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\EMDMgmt\<disk&ven-driveID-Vol>

SOFTWARE – Startup Software.rsr

- Global startup software for any user who logs on is stored in the SOFTWARE file. For per user settings, see the NTUSER.DAT file. There are many other locations in the Registry in which startup software can be initiated during bootup or during startup of other utilities.
- HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run (RunServices)

SYNTRICATE

Registry Summary Reports

Dustin Hurlbut

For more information contact: info@syntricate.com

SOFTWARE – Time Synch Server Used.rsr

- The address below provides an MRU list of time servers used and the current one being used in the Default value. See the SYSTEM file for whether time synch is in use and the period of synchronization.

- HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\DateTime\Servers

SOFTWARE – User and OS.rsr

- This keyset displays two types of information; installed operating system information and data entered by the user upon installation of the system

- HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion

SOFTWARE – Vista Security Settings.rsr

- This RSR records the Vista Security settings for the User Access Control of the target system. It will also archive any captions added by the user for logon purposes.

- HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System / EnableLUA (default is 1 = On, the value of 0 turns off the UAC)

SOFTWARE – Vista Wireless.rsr

- Vista wireless SSID connections are retrieved with this RSR and include the network profiles list which lists connections in wireless and the Signatures subkey that records managed and unmanaged connections.

- HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Profiles and Signatures

SYNTRICATE

Registry Summary Reports

Dustin Hurlbut

For more information contact: info@syntricate.com

SOFTWARE – Winlogon.rsr

- The Winlogon RSR records information stored in the Winlogon subkey such as legal notices, cached logons count, and if enabled, autologon information like user name, domain name, and password used.

- HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon

SOFTWARE – XP Recycle Bin Settings.rsr

- The XP Recycle Bin settings captured include global settings and individual drive settings. Included values are: drive settings and volume serial number.

- HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\BitBucket

SOFTWARE – XP Wireless Network Connections.rsr

- There are two potential XP locations for identifying SSID connections from the target system. Both list the SSID name of the connection, however little other information is available. WZCSVC is written to if using the built in Windows wireless service. EAPOL is used if using the Extensible Authentication Protocol for connection. If other wireless systems are used, information may or may not be available in the Registry.

- HKLM\SOFTWARE\Microsoft\WZCSVC\Parameters\Interfaces\<guid> / Static#000n

- HKLM\SOFTWARE\Microsoft\EAPOL\Parameters\Interfaces\<guid> / n

SYNTRICATE

Registry Summary Reports

Dustin Hurlbut

For more information contact: info@syntricate.com

SYSTEM File RSRs

SYSTEM – Clearing Paged Memory.rsr

- This RSR reports whether the ability to wipe active page files on shutdown has been activated.
- HKLM\ControlSet###\Control\Session Manager\Memory Management / ClearPageFileAtShutdown (Default Off=0, On=1)

SYSTEM – Computer Name.rsr

- Computer name recovers the computer name of the system.
- HKLM\SYSTEM\ControlSet###\Control\ComputerName\ComputerName

SYSTEM – Last Shutdown Time.rsr

- This RSR recovers the last normal shutdown of the system in XP, and in Vista SP1. It did not appear in the first Vista release.
- HKLM\SYSTEM\ControlSet###\Control\Windows / ShutdownTime

SYSTEM – MountedDevices.rsr

- The Mounted Devices RSR captures mounted drive information in the SYSTEM file. It is best run with the option of "Reduce excess data output to limit the recovered binary data. With this option, it recovers the volatile USB attached drives, drive letters, and the persistent archives as well.
- HKLM\SYSTEM\MountedDevices\<driveletters and guids>

SYNTRICATE

Registry Summary Reports

Dustin Hurlbut

For more information contact: info@syntricate.com

SYSTEM – Prefetch Settings.rsr

- The Prefetch RSR records the Prefetch setting for the system and the path to where the Prefetch files are located)
- HKLM\SYSTEM\ControlSet###\Control\Session Manager\Memory Management\PrefetchParameters / EnablePrefetcher

SYSTEM – Select Key.rsr

- This RSR identifies the Select key setting used upon shutdown.
- HKLM\SYSTEM\Select / Current

SYSTEM – Startup Software.rsr

- The SYSTEM Startup RSR archives the settings for BootExecute which can initiate applications during the boot process.
- HKLM\SYSTEM\ControlSet###\Control\Session Manager / BootExecute

SYSTEM – Time Synch Enabled.rsr

- The SYSTEM RSR for automatic time synchronization records whether the system is auto synching (NTP=Yes, NoSync=No) and the update interval (default=0x093A80 or decimal 604800 which is exactly 7 days in seconds).
- HKLM\SYSTEM\CurrentControlSet\Services\W32Time\TimeProviders\NtpClient\

SYSTEM – Vista File System Information.rsr

- This RSR obtains two key Vista properties about the file system; whether Disable Last Access Update is turned on and whether encrypt the page file was turned on.
- HKLM\SYSTEM\CurrentControlSet\FileSystem

SYNTRICATE

Registry Summary Reports

Dustin Hurlbut

For more information contact: info@syntricate.com

SYSTEM – Vista Time Zone Settings.rsr

- This RSR records the current time zone settings of the Vista system, different than XP.

- HKLM\SYSTEM\ControlSet###\Control\TimeZoneInformation

SYSTEM – XP Time Zone Settings.rsr

- The XP Time Zone Settings RSR captures the XP time zone settings, different than Vista.

- HKLM\SYSTEM\ControlSet###\Control\TimeZoneInformation

Document Conventions

Hexadecimal numbers are indicated with a 0x prefix; i.e.: the hex number FFFF will be shown as 0xFFFF.

Hex numbers may use both upper and lower case letters. They are generally presented as they are shown in the software examined or to the tool being used. For example, 0xffff is the same as 0xFFFF.

Decimal numbers are defined by either a 0d, “decimal”, or with no signature.

When referring to registry root keys, the abbreviation HKLM is used to signify the Microsoft use of HKEY_LOCAL_MACHINE.

Paths in the registry will begin with the registry filename the data is contained in. The filename will be in uppercase. This is to distinguish between filename used by Registry Viewer and hive names used by Microsoft’s Regedit. For example, the following path is from the NTUSER.DAT file. The same path follows if using the Regedit addressing system:

NTUSER.DAT\Software\Microsoft\Internet Explorer\TypedURLs

HKCU\Software\Microsoft\Internet Explorer\TypedURLs

Registry Summary Reports

Dustin Hurlbut

For more information contact: info@syntricate.com

Paths in the Registry are shown using backslashes to divide the keys and subkeys. However, if a value name is at the end of the path, it will be denoted with a forward slash. For example the value name "TestValue" would be shown as follows:

NTUSER\Software\Microsoft\Windows\CurrentVersion / TestValue

If general numbers are being expressed, like value sets that contain sequential numbers, the number will be expressed with an "n" notation to mean any number.

Numbers like 0001, 0002, 0003, etc. will be expressed as 000n or nnnn.

Disclaimer

As with most registry content knowledge, this information is based upon the author's research. While described behavior has been found to be consistent, different platforms and user configurations may produce different results. Anyone with additional information or differing behavior is urged to contact the author so that updates and additional research can be conducted.

SYNTRICATE