ACCESSDATA SUPPLEMENTAL APPENDIX

Registry Quick Find Chart

Important: At the time of this writing, most of the information contained in this paper is not published by Microsoft and is based on personal research. As such, please consider validating these results prior to relying on them as the basis for any conclusions. Please keep in mind that, as with all Windows artifact behavior, the information contained in this paper is subject to change at any time. In addition to the conditions stated below, there may be additional user actions that may contribute to these entries.

This appendix reviews common locations in the Windows and Windows Internet-related registries where you can find data of forensic interest.

Note: Under the Version column, an "XP" indicates that this information is found in XP. A "V" references Vista, and a "7" references Windows 7 in its first release. If no notation is made in the Version column, it means this was found in XP, but not tested in other versions.

NTUSER.DAT Information

Information	File	Location	Description	When Updated	Version
Access 2007 MRU	NTUSER.DAT	NTUSER.DAT\Software\Microsoft\Office\12.0\Access\ Settings	MRU list for MS Access Database files (MRU1-MRU9).	When database is closed	Office 2007
Access 2007 MRU Dates	NTUSER.DAT	NTUSER.DAT\Software\Microsoft\Office\12.0\Access\Settings	Tracks date of last access associated with MRU1-9 (MRUDate1-MRUDate9).	When database is closed	Office 2007
Access Recent Databases	NTUSER.DAT	NTUSER.DAT\Software\Microsoft\office*version*\ Common\Open Find\ Microsoft Office Access\Settings\ File New Database\File Name MRU	Microsoft Access* recent databases in the "value" value.	Immediately	Pre Office 2007
Adobe	NTUSER.DAT	NTUSER.DAT\Software\Adobe*	Lists Adobe products such as Acrobat* and FrameMaker*.		
AIM	NTUSER.DAT	NTUSER.DAT\Software\America Online\AOL InstantMessenger\ CurrentVersion\Users\ *username*	Lists IM contacts, file transfer information, etc.	Immediately	
AIM Away Messages	NTUSER.DAT	NTUSER.DAT\Software\America Online\AOL Instant Messenger(TM)\ CurrentVersion\Users\screen name\ IAmGoneList	Shows default and customized Away messages.	Immediately	
AIM File Transfers & Sharing	NTUSER.DAT	NTUSER.DAT\Software\America Online\AOL Instant Messenger\ CurrentVersion\Users\screen name\ Xfer	Shows settings for file transfers and sharing.	Immediately	

Information	File	Location	Description	When Updated	Version
AIM Last User	NTUSER.DAT	NTUSER.DAT\Software\America Online\AOL Instant Messenger (TM)\ CurrentVersion\Login - Screen Name	Shows the screen name of the last logged-in user.	At login	
AIM Profile Info	NTUSER.DAT	NTUSER.DAT\Software\America Online\AOL Instant Messenger\ CurrentVersion\Users\screen name\DirEntry	Shows user profile information (optional).	Immediately	
AIM Recent Contacts	NTUSER.DAT	NTUSER.DAT\Software\America Online\AOL Instant Messenger\ CurrentVersion\users\ username\ recent IM ScreenNames	Shows a list of recently contacted buddies.	When the application closes.	
AIM Registered Users	NTUSER.DAT	NTUSER.DAT\Software\America Online\AOL Instant Messenger\ CurrentVersion\Users	Shows registered AIM users on the machine.	At sign-on	
AIM Saved Buddy List	NTUSER.DAT	NTUSER.DAT\Software\America Online\AOL Instant Messenger\ CurrentVersion\Users\username\Config Transport	Shows the directory path of a saved Buddy List, a BLT file.	Immediately	
Application Information	NTUSER.DAT	NTUSER.DAT\Software\%Application Name%	This class of registry keys contains the information each application stores in the registry.	NA	
Autorun USBs, CDs, DVDs	NTUSER.DAT	NTUSER.DAT\Software\Microsoft\ Windows\ CurrentVersion\Explorer\ AutoplayHandlers / DisableAutoplay	0=Enabled 1=Disabled	N/A	XP, V

Information	File	Location	Description	When Updated	Version
BitLocker To Go	NTUSER.DAT	NTUSER.DAT\Software\Microsoft\ Windows\CurrentVersion\ FveAutoUnlock\<guid>	Indicates the user-selected **Remember a USB** setting to bypass entering the password on this system.	Upon selecting, recognize the drive on this machine	7
CD Burning	NTUSER.DAT	NTUSER.DAT\Software\Microsoft\ Windows\CurrentVersion\Explorer\ CD Burning\Drives\Volume<guid>\ Current Media	May show previous CD/DVD volume names inserted under Disc Label value. Normally, removes volume name on dismount.	N/A	V, 7
CD Burning	NTUSER.DAT	NTUSER.DAT\Software\Microsoft\ Windows\CurrentVersion\Explorer\ CD Burning\ Current Media / Disc Label	Current Media subkey created upon mounting drive. Removed on dismount.	Upon mounting and dismounting	XP
Chat Rooms	NTUSER.DAT	NTUSER.DAT\Software\Yahoo\Pager\ profiles*screen name*\Chat	Shows information for chat rooms visited or created.	Immediately	
Converted Wallpaper	NTUSER.DAT	NTUSER.DAT\\Control Panel\Desktop	Identifies graphics that are converted to wallpaper.	Immediately	XP, V, 7
Converted Wallpaper	NTUSER.DAT	NTUSER.DAT\\Control Panel\Desktop	Identifies date and time of converted wallpaper.	Immediately	XP, V, 7
Drives mounted by user	NTUSER.DAT	NTUSER.DAT\Software\Microsoft\ Windows\ CurrentVersion\Explorer\ MountPoints2\<guid>	Track the GUID from the MountedDevices GUID in the SYSTEM file	Immediately	XP, V, 7

Information	File	Location	Description	When Updated	Version
EFS	NTUSER.DAT	NTUSER.DAT\Software\Microsoft\ WindowsNT\CurrentVersion\EFS\ CurrentKeys	Lists the current user's certificate thumbprint. (Each user has a unique certificate thumbprint.) The same certificate thumbprint is contained in the $EFS alternate data stream for every EFS file encrypted by the current user.	NA	XP, V, 7
Excel 2007 Autosave Info	NTUSER.DAT	NTUSER.DAT\Software\Microsoft\ Office\12.0\Excel\ Resiliency\ Document Recovery\<id#>	Saves info about currently opened Excel documents.	When document is opened and when saves are made	Office 2007
Excel 2007 MRU	NTUSER.DAT	NTUSER.DAT\Software\Microsoft\ Office\12.0\Excel\ File MRU	MRU List for MS Excel spreadsheets (Item1-Item50). **Note:** The 2nd bracketed number is a 64-bit date/time stamp of when the document was opened.	When document is opened	Office 2007
Excel Recent Spreadsheets	NTUSER.DAT	NTUSER.DAT\Software\Microsoft\ office*version*\ Common\Open Find\ Microsoft Office Excel\Settings\ Save As\File Name MRU	Microsoft Excel recent spreadsheets in the "value" value.	Immediately	Pre Office 2007
File Extension Associations	NTUSER.DAT	NTUSER.DAT\Software\Microsoft\ Windows\ CurrentVersion\Explorer\ FileExts\.*EXT Type*	Lists file extension associations and files that have been opened with the Open With command.	Immediately	XP, V, 7
File Extensions\ Program Association	NTUSER.DAT	NTUSER.DAT\Software\Microsoft\ Windows\CurrentVersion\Explorer\ FileExts	Identifies associated programs with file extensions.	Immediately	XP, V, 7

Information	File	Location	Description	When Updated	Version
Folders - Stream MRUs	NTUSER.DAT	NTUSER.DAT\Software\Microsoft\ Windows\ CurrentVersion\ Explorer\StreamMRU	Info on stored folders.	Immediately	XP
FTP	NTUSER.DAT	NTUSER.DAT\Software\Microsoft\FTP\ Accounts\ <address>	Local FTP accounts.	N/A	XP, V, 7
Google Client History	NTUSER.DAT	NTUSER.DAT\Software\Google\ NavClient\1.1\History	Contains a list of search terms with date and time stamps if Google is included in the Internet Explorer task bar.	Immediately	
ICQ	NTUSER.DAT	NTUSER.DAT\Software\Mirabilis\ICQ*	Lists IM contacts, file transfer information, etc.	NA	
ICQ Last User	NTUSER.DAT	NTUSER.DAT\Software\Mirabilis\ICQ\ Owners - LastOwner	Shows the last logged-in user.	At logon	
ICQ Nickname	NTUSER.DAT	NTUSER.DAT\Software\Mirabilis\ICQ\ Owners\UIN - Name	Nickname of user (optional value).	At logon	
ICQ Registered Users	NTUSER.DAT	NTUSER.DAT\Software\Mirabilis\ICQ\ Owners\UIN	UIN folder is named for the user.	At logon	
IE Auto Logon and password	NTUSER.DAT	NTUSER.DAT\Software\Microsoft\ Protected Storage System Provider\ SID\Internet Explorer\Internet Explorer - URL: StringData	Stores IE auto logon IDs and passwords with date and time stamp.	Immediately	IE6 and below
IE Auto–Complete Passwords	NTUSER.DAT	NTUSER.DAT\Software\Microsoft\ Internet Explorer\IntelliForms	Stores web page auto-complete passwords. These are encrypted values.	Immediately	IE6 and below

Information	File	Location	Description	When Updated	Version
IE Auto–Complete Web Addresses	NTUSER.DAT	NTUSER.DAT\Software\Microsoft\ Protected Storage System Provider	Lists web pages wherein autocomplete was utilized.	Immediately	IE6 and below
IE Cleared Browser History on/off	NTUSER.DAT	NTUSER.DAT\Software\Microsoft\ Internet Explorer\ Privacy / ClearBrowserHistoryOnExit	0=Off (default) 1=On Privacy subkey appears only on first change by user.	Upon changing value in GUI	XP, V, 7
IE Default Download Directory	NTUSER.DAT	NTUSER.DAT\Software\Microsoft\ Internet Explorer	Identifies the default download directory when utilizing Internet Explorer.	Immediately	All
IE Favorites List	NTUSER.DAT	NTUSER.DAT\Software\Microsoft\ Windows\CurrentVersion\Explorer\ MenuOrder\ Favorites\ <favoritesfoldername>	Lists favorites from IE Favorites drop down selector.	N/A	XP, V, 7
IE History Status	NTUSER.DAT	NTUSER.DAT\Software\Microsoft\ Windows\ CurrentVersion\Internet Settings\ 5.0\Cache\Extensible Cache\ <mshistfoldernames>	Mirrors existing history folder storage hidden from the user in the history files.	N/A	XP, V, 7
IE IntelliForms	NTUSER.DAT	NTUSER.DAT\Software\Microsoft\ Internet Explorer\ IntelliForms	Encrypted user data in Storage1 and Storage2 (old PSSP info)		IE7 and above
IE Search Terms	NTUSER.DAT	NTUSER.DAT\Software\Miscrosoft\ Protected Storage System Provider\ SID\Internet Explorer\ Internet Explorer - q:StringIndex	Stores IE search terms with date and time stamp.	Immediately	IE6 and below

Information	File	Location	Description	When Updated	Version
IE Settings	NTUSER.DAT	NTUSER.DAT\Software\Microsoft\ Internet Explorer\ Main	Stores IE settings such as start page, save directory, home page, and download location.	Immediately	Through IE8
IE Typed URLs	NTUSER.DAT	NTUSER.DAT\Software\Microsoft\ Internet Explorer\Typed URLs	Stores data entered into the URL Address Bar.	When the application closes	Through IE8
IE URL History — Days Saved	NTUSER.DAT	NTUSER.DAT\Software\Microsoft\ Windows\CurrentVersion\Internet Settings\URL History - DaysToKeep	The number of days the system stores URLs visited in IE. The default is 20 days.	Immediately	Through IE8
IE Web Form Data	NTUSER.DAT	NTUSER.DAT\Software\Microsoft\Protected Storage System Provider\SID\ Internet Explorer\Internet Explorer - q:StringIndex	Stores form data provided within IE.	Immediately	IE6 and below
IM Contact List	NTUSER.DAT	NTUSER.DAT\Software\Microsoft\ MessengerService\ListCache\.NET Messenger Service	Contains Contact, Allow, Block, and Reverse entries.	At sign-off	
IM File Sharing	NTUSER.DAT	NTUSER.DAT\Software\Microsoft\ MSNMessenger\FileSharing - Autoshare	Shows if file sharing is turned on.	Immediately	
IM File Transfers	NTUSER.DAT	NTUSER.DAT\Software\Microsoft\ Messenger Service - FtReceiveFolder	Shows the location of the Received Files folder.	Immediately	
IM File Transfers	NTUSER.DAT	NTUSER.DAT\Software\Microsoft\ MSNMessenger\- FTReceiveFolder	Shows the location of the Received Files folder.	Immediately	
IM Last User	NTUSER.DAT	NTUSER.DAT\Software\Microsoft\ MessengerService\ListCache\.NET Messenger Service - IdentityName	Screen name of last logged-in user.	At sign-off	

Information	File	Location	Description	When Updated	Version
IM Logging Enabled	NTUSER.DAT	NTUSER.DAT\Software\Microsoft\MSN Messenger\PerPass portSettings\ ##########\- MessageLoggingEnabled	Shown if message logging is turned on.	Immediately	
IM Message History	NTUSER.DAT	NTUSER.DAT\Software\Microsoft\MSN Messenger\PerPass portSettings\ ##########\- MessageLog Path	Shows the location of message history files.	Immediately	
IM MSN Messenger	NTUSER.DAT	NTUSER.DAT\Software\Microsoft MessengerService\ ListCache\.NET MessngerService*	Contains IM groups, contacts, file transfer information, etc. for MSN Messenger.	Most on signoff; however, FTReceive is immediate.	
IM Saved Contact List	NTUSER.DAT	NTUSER.DAT\Software\Microsoft\ Messenger Service - ContactListPath	Shows the location of a saved Contact List (CTT) file.	Immediately	
IMV Usage	NTUSER.DAT	NTUSER.DAT\Software\Yahoo\Pager\ IMVironments (global value)	Shows usage of IMVironments.	Immediately	
IMVs MRU list	NTUSER.DAT	SNTUSER.DAT\oftware\Yahoo\Pager\ profiles\screen name\IMVironments (user- specific value)	Shows usage of IMVironments.	Immediately	
Jump List on Taskbar	NTUSER.DAT	NTUSER.DAT\Software\Microsoft\ Windows\ CurrentVersion\Explorer\ Taskband / Favorites and FavoritesResolve	Shows applications pinned to the taskbar. Retains removed applications.	Upon pinning	7
Kazaa	NTUSER.DAT	NTUSER.DAT\Software\Kazaa*	Stores configuration, search, download, IM data, etc. for Kazaa.	NA	
Map Network Drive MRU	NTUSER.DAT	NTUSER.DAT\Software\Microsoft\ Windows\CurrentVersion\Explorer\ Map Network Drive MRU	Contains a most recently used list of mapped network drives.	NA	XP, V, 7

Information	File	Location	Description	When Updated	Version
Media Player Recent List	NTUSER.DAT	NTUSER.DAT\Software\Microsoft\ MediaPlayer\Player\ RecentFileList	Contains the user's most recently used list for Windows Media Player.	Immediately	
MRU—Last Visited	NTUSER.DAT	NTUSER.DAT\Software\Microsoft\ Windows\CurrentVersion\Explorer\ ComDlg32\	Lists the application and filename of the most recent files opened in Windows.	Immediately	XP, V, 7
MRU—Open Saved	NTUSER.DAT	NTUSER.DAT\Software\Microsoft\ Windows\ CurrentVersion\Explorer\ ComDlg32\OpenSaveMRU	Lists the filename and path of the most recent files saved or copied to a specific location in Windows.	Immediately	XP, V, 7
MRU— Recent Documents	NTUSER.DAT	NTUSER.DAT\Software\Microsoft\ Windows\ CurrentVersion\Explorer\ RecentDocs\	Identifies the documents in the Recent Documents list available from the Windows Start menu.	Immediately	XP, V, 7
MRU—Run MRU	NTUSER.DAT	NTUSER.DAT\Software\Microsoft\ Windows\CurrentVersion\Explorer\ RunMRU	Lists the most recent commands entered in the Windows Run box.	Immediately	XP, V, 7
MRUs - Common Dialog	NTUSER.DAT	NTUSER.DAT\Software\Microsoft\ Windows\ CurrentVersions\Explorer\ ComDlg32	Last Visited=Application Used OpenSaveMRU=Recent Docs using the Microsoft Save As Dialog Box	Immediately	XP, V, 7
MUICache	NTUSER.DAT	NTUSER.DAT\Software\Microsoft\ Windows\Shell\MUICache	Tracks the opening of executable files by the operating system. **Note:** In Windows 7, MUICache moved from NTUSER.DAT to HKCR\LocalSettings\MuiCache.	Immediately	V
MUICache - XP	NTUSER.DAT	NTUSER.DAT\Software\Microsoft\ Windows\ShellNoRoam\MUICache	Tracks the opening of executable files by the operating system	Immediately	XP

Information	File	Location	Description	When Updated	Version
Network - Computer Description	NTUSER.DAT	NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\ComputerDescriptions	Network connections	N/A	
Network - Mapped Network Drive MRU	NTUSER.DAT	NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\Map Network Drive MRU	Listed by drive letter	Immediately	XP, V, 7
Network - Workgroup Crawler	NTUSER.DAT	NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\WorkgroupCrawler\Shares	Network connections crawled while connected.	N/A	
Outlook Account Passwords	NTUSER.DAT	NTUSER.DAT\Software\Microsoft\Protected Storage SystemProvider\SID\Identification\INETCOMM Server Passwords	Stores Outlook and Outlook Express account passwords.	Immediately	
Outlook Recent Attachments	NTUSER.DAT	NTUSER.DAT\Software\Microsoft\office*version*\Common\Open Find\Microsoft Office Outlook\Settings\Save Attachment\File Name MRU	Microsoft Outlook recent documents.	Immediately	
Outlook Temporary Attachment Directory	NTUSER.DAT	NTUSER.DAT\Software\Microsoft\Office*version*\Outlook\Security	Identifies the location where attachments are stored when they are opened from Outlook.	Immediately	
Paint MRU	NTUSER.DAT	NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Applets\Paint\Recent File List	MRU for MS Paint documents (File1-File9)	Upon closing the application	XP, V, 7

Information	File	Location	Description	When Updated	Version
POP3 Passwords	NTUSER.DAT	NTUSER.DAT\Software\Microsoft\ Internet Account Manager\Accounts\ 0000000#	Identifies the current user's POP3 passwords. **Note:** # is a digit identifying that particular account.	Immediately	XP
PowerPoint 2007 Autosave Info	NTUSER.DAT	NTUSER.DAT\Software\Microsoft\ Office\12.0\ PowerPoint\Resiliency\ DocumentRecovery\<id#>	Saves info about currently opened PowerPoint documents.	When document is opened and when saves are made	Office 2007
PowerPoint 2007 MRU	NTUSER.DAT	SNTUSER.DAT\oftware\Microsoft\ Office\12.0\ PowerPoint\File MRU	MRU List for MS PowerPoint spreadsheets (Item1-Item50). **Note:** The second bracketed number is a 64-bit date/time stamp of when the document was opened.	When document is opened	Office 2007
PowerPoint—Recent PPTs	NTUSER.DAT	NTUSER.DAT\Software\Microsoft\ office*version*\ Common\Open Find\ Microsoft Office PowerPoint\Settings\ Save As\File Name MRU	Microsoft PowerPoint recent documents.	Unknown	Pre Office 2007
Printer—Default	NTUSER.DAT	NTUSER.DAT\Software\Microsoft\ WindowsNT\CurrentVersion\Windows	Identifies the current default printer.	Immediately	XP, V, 7
Printer—Default	NTUSER.DAT	NTUSER.DAT\\printers	Identifies the current default printer.	On shutdown	XP, V, 7

Information	File	Location	Description	When Updated	Version
Publisher 2007 MRU	NTUSER.DAT	NTUSER.DAT\Software\Microsoft\Office\12.0\Publisher\Recent File List	MRU List for MS Publisher documents (File1-File9).	When document is opened	Office 2007
Publisher—Recent Documents	NTUSER.DAT	NTUSER.DAT\Software\Microsoft\office*version*\Common\Open Find\Microsoft Office Publisher\Settings\Save As\File Name MRU	Microsoft Publisher recent documents.	Unknown	Pre Office 2007
Recycle Bin Info	NTUSER.DAT	NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\BitBucket\Volume\<guid>	Tracks recycle bin info by GUID (track GUID back to MountedDevices in the SYSTEM file), Max Capacity in MB, NukeOnDelete. 0=Bin being used (default) 1= Bin is being bypassed	N/A	V, 7
Regedit - Favorites	NTUSER.DAT	NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Applets\Regedit\Favorites	Displays user selected favorites in Regedit Utility.	Immediately after entering	XP, V, 7
Regedit - Last Key Saved	NTUSER.DAT	NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Applets\Regedit / LastKey	Displays last subkey Regedit was on when closed down	Upon closing Regedit.	XP, V, 7
Run	NTUSER.DAT	NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Run	Lists programs that run automatically when the user logs on.	NA	XP, V, 7

Information	File	Location	Description	When Updated	Version
Screen Saver Enabled	NTUSER.DAT	NTUSER.DAT\Control Panel\Desktop / ScreenSaveActive	1=Active 0=Disabled The path/name displays at SCRNSAVE.EXE. **Note:** In Windows 7, ScreenSaveActive retains a 1 whether enabled or not, but the path/name appears on enable and disappears on disable.	Immediately	XP, V, 7
Screen Saver Password Enabled	NTUSER.DAT	NTUSER.DAT\Control Panel\Desktop / ScreenSaverIsSecure	0=No Password Required 1=Password Required if screen saver is active	Immediately	XP, V, 7
Screen Saver Timeout	NTUSER.DAT	NTUSER.DAT\Control Panel\Desktop / ScreenSaveTimeOut	Length of time, in seconds, before the screen saver becomes active.	Immediately	XP, V, 7
Screen Savers and wallpaper	NTUSER.DAT	NTUSER.DAT\Control Panel\Desktop\	Identifies the system's screen saver and wallpaper.	Immediately	XP, V, 7
ShellBags	NTUSER.DAT	NTUSER.DAT\Software\Microsoft\ Windows\Shell\ BagMRU	Pointers to link history and other file and folder information.	NA	XP
Start Menu Program List	NTUSER.DAT	NTUSER.DAT\Software\Microsoft\ Windows\CurrentVersion\Explorer\ MenuOrder\ Programs\<appname>	Program listing drawn to the Start button.	N/A	XP

Information	File	Location	Description	When Updated	Version
Start Searches entered by user	NTUSER.DAT	NTUSER.DAT\Software\Microsoft\ Windows\ CurrentVersion\Explorer\ WordWheelQuery	In Windows 7, traps search terms entered by the user in the Start > Search box.	After hitting the enter button.	7
Start Searches entered by user	NTUSER.DAT	NTUSER.DAT\Software\Microsoft\ SearchAssistant\ ACMru\<5###>	Searches from the built-in search engine. 5001=Internet Searches 5603=Files and Folders 5604=Pictures and Music 5647=Computers and People	Immediately	XP
Startup Software	NTUSER.DAT	NTUSER.DAT\Software\Microsoft\ Windows\ CurrentVersion\Run	Stores the applications automatically launched at boot time. This key is a good place to look for trojans.	NA	XP, V, 7
Startup Software	NTUSER.DAT	NTUSER.DAT\Software\Microsoft\ Windows\CurrentVersion\RunOnce	Stores the applications automatically launched at boot time. This key is a good place to look for trojans.	NA	XP, V, 7
Theme—Current Theme	NTUSER.DAT	NTUSER.DAT\Software\Microsoft\ Windows\CurrentVersion\Themes	Identifies the Desktop theme and wallpaper.	Unknown	XP, V, 7
Theme—Last Theme	NTUSER.DAT	NTUSER.DAT\Software\Microsoft\ Windows\CurrentVersion\Themes\ Last Theme	Identifies the Desktop theme and wallpaper.	Immediately	XP, V
Type Paths into Windows Explorer	NTUSER.DAT	NTUSER.DAT\Software\Microsoft\ Windows\CurrentVersion\Explorer\ TypedPaths	User typed (or pasted) paths into Windows Explorer address bar	Upon hitting <Enter>.	7

Information	File	Location	Description	When Updated	Version
UserAssist	NTUSER.DAT	NTUSER.DAT\Software\Microsoft\ Windows\ CurrentVersion\Explorer\ UserAssist\<guid>	Application usage showing last access and number of launches of applications. **Note:** GUID 750 is used in versions 2000, XP, and Vista.	Immediately	XP, V
UserAssist	NTUSER.DAT	NTUSER.DAT\Software\Microsoft\ Windows\CurrentVersion\Explorer\ UserAssist\ <guid>	Application usage showing last access and number of launches of applications. **Note:** Change to GUID F4E in Windows 7 for application launch info.	Immediately	7
Windows Explorer Settings	NTUSER.DAT	NTUSER.DAT\Software\Microsoft\ Windows\ CurrentVersion\Explorer\ Advanced	Sets Windows Explorer preferences.	Immediately	XP, V, 7
WinZip - Accessed Archives	NTUSER.DAT	NTUSER.DAT\Software\Nico Mak Computing\filemenu / filemenu##	Path back to accessed Zip archives	Immediately	11.1
WinZip - Extraction MRU	NTUSER.DAT	NTUSER.DAT\Software\Nico Mak Computing\ Extract / extract#	The path to which Zip archives are extracted.	Immediately	11.1
WinZip - Location Extracted To	NTUSER.DAT	NTUSER.DAT\Software\Nico Mak Computing\ Directories / ExtractTo	Last location to which a Zip archive was extracted.	Immediately	11.1
WinZip - Registered User	NTUSER.DAT	NTUSER.DAT\Software\Nico Mak Computing\ WinIni / Name 1	Registered user for installation	N/A	11.1

Information	File	Location	Description	When Updated	Version
WinZip - Temp File	NTUSER.DAT	NTUSER.DAT\Software\Nico Mak Computing\Directories / ZipTemp	WinZip temporary file location	N/A	11.1
WinZip - Zip Creation Location	NTUSER.DAT	NTUSER.DAT\Software\Nico Mak Computing\Directories / AddDir	Last location from which a Zip file was created.	Immediately	11.1
WinZip - Zip Creation Location	NTUSER.DAT	NTUSER.DAT\Software\Nico Mak Computing\Directories / DefDir	Last location to which a Zip file was created or opened.	Immediately	11.1
Word 2007 Autosave Info	NTUSER.DAT	NTUSER.DAT\Software\Microsoft\Office\12.0\Word\Resiliency\Document Recovery\<id#>	Saves info about currently opened Word documents.	When document is opened and when saves are made	Office 2007
Word 2007 MRU	NTUSER.DAT	NTUSER.DAT\Software\Microsoft\Office\12.0\Word\File MRU	MRU List for MS Word documents (Item1-Item50). **Note:** The second bracketed number is a 64-bit date/time stamp of when document was opened.	When document is opened	Office 2007
Word—Recent Docs	NTUSER.DAT	NTUSER.DAT\Software\Microsoft\office*version*\Common\Open Find\Microsoft Office\Word\Settings\Save As\File Name MRU	Microsoft Word recent documents in the “value” value.	Unknown	Pre Office 2007
Word—User Info	NTUSER.DAT	NTUSER.DAT\Software\Microsoft\office*version*\Common\UserInfo	Identifies the user information entered when installing Microsoft Office. Note this information may be modified after installation.	Unknown	Pre Office 2007

Information	File	Location	Description	When Updated	Version
WordPad MRU	NTUSER.DAT	NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Applets\Wordpad\Recent File List	MRU for MS Paint documents (File1-File9).	When document is closed	XP, V, 7
Yahoo!	NTUSER.DAT	NTUSER.DAT\Software\Yahoo\Pager\Profiles*	Stores IM contacts, file transfer information, etc. for Yahoo!.	NA	
Yahoo! File Transfers	NTUSER.DAT	NTUSER.DAT\Software\Yahoo\Pager\File Transfer (global value)	Shows number of transfers in and out.	Immediately	
Yahoo! File Transfers	NTUSER.DAT	NTUSER.DAT\Software\Yahoo\Pager\profiles*screen name*\FileTransfer (user specific)	Shows settings for file transfers.	Immediately	
Yahoo! Identities	NTUSER.DAT	NTUSER.DAT\Software\Yahoo\Pager\profiles\screen name - All Identities, Selected Identities	Shows alternate user identities.	Unknown	
Yahoo! Last User	NTUSER.DAT	NTUSER.DAT\Software\Yahoo\Pager - Yahoo! User ID	Last logged-in user.	Immediately	
Yahoo! Message Archiving	NTUSER.DAT	NTUSER.DAT\Software\Yahoo\Pager\profiles*screen name*\Archive	Shows settings for message archiving.	Immediately	
Yahoo! Password	NTUSER.DAT	NTUSER.DAT\Software\Yahoo\Pager - EOptions string	Encrypted password.	Immediately	
Yahoo! Recent Contacts	NTUSER.DAT	NTUSER.DAT\Software\Yahoo\Pager\profiles\screen name\IMVironments\Recent	Shows recent contacts and which IMV was used.	Immediately	
Yahoo! Saved Password	NTUSER.DAT	NTUSER.DAT\Software\Yahoo\Pager - Save Password	Shows if the password is saved.	Immediately	

Information	File	Location	Description	When Updated	Version
Yahoo! Screen Names	NTUSER.DAT	NTUSER.DAT\Software\Yahoo\Pager\profiles*screen name*	Shows registered screen names and identities.	Immediately	
Yserver	NTUSER.DAT	NTUSER.DAT\Software\Yahoo\Yserver	Points to a directory location for file transfer information.	NA	

SAM Information

Information	File	Location	Description	When Updated	Version
Account Expiration	SAM	SAM\Domains\Account\Users\F Key	Bytes 33-40 store the account expiration. If no expiration is set, FF FF FF FF shows.	NA	XP, V, 7
Group Names - Custom	SAM	SAM\Domains\Account\Aliases\Names	List of custom groups by name.	Immediately	XP, V, 7
Group Names - Local	SAM	SAM\Domains\Builtin\Aliases\Names	List of local group names.	Immediately	XP, V, 7
Groups - Custom	SAM	SAM\Domains\Account\Aliases\<rid>	List of custom groups by RID.	Immediately	XP, V, 7
Groups - Local	SAM	SAM\Domains\Builtin\Aliases\<rid>	Listed of local groups by RID.	Immediately	XP, V, 7
Home Group	SAM	SAM\SAM\Domains\Account\Users - Home Group in RID and Names		N/A	7
Last Failed Login	SAM	SAM\Domains\Account\Users\F Key	Bytes 41-48 store the last unsuccessful logon.	NA	XP, V, 7
Last Logon Time	SAM	SAM\Domains\Account\Users\F Key	Bytes 9–16 store the last log-on time.	NA	XP, V, 7

Information	File	Location	Description	When Updated	Version
Last Time Password Changed	SAM	SAM\Domains\Account\Users\F Key	Bytes 25–32 store the last time the password was changed.	NA	XP, V, 7
Local Groups	SAM	SAM\Domains\Builtin\Aliases\Names	Lists local account security identifiers.	NA	XP, V, 7
Local Users	SAM	SAM\Domains\Account\Users\Names	Lists local account security identifiers.	NA	XP, V, 7
Machine SID Location	SAM	SAM\Domains\Account / V	Last twelve bytes of the V value.	N/A	XP, V, 7
Password Hint	SAM	SAM\Domains\Account\Users\<*RID*>\ *F_Value*\UserPasswordHint	Shows a logon password hint if initiated by the user		V, 7
User Name and SID	SAM	SAM\Domains\Account\Users\V Key **Note:** See "User Name and SID" in *SOFTWARE Information* on page 21.	Contains the username and SID in hex. You must convert the last three hex numbers to decimal to determine the decimal version of the SID that is used in the Recycler and System Volume Information folder.	NA	XP, V, 7

SECURITY Information

Information	File	Location	Description	When Updated	Version
Passwords—Cached Administrative Passwords	SECURITY	SECURITY\Policy\Secrets\DefaultPassword / CurrVal and OldVal	CurrVal holds the current administrative password and OldVal holds the previous.	N/A	XP, 7
Passwords—Cached Domain Passwords	SECURITY	SECURITY\Cache / NL$#	Default stores up to 10 set in SOFTWARE file.	N/A	XP

SOFTWARE Information

Information	File	Location	Description	When Updated	Version
Auto Logon Set	SOFTWARE	SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon / AutoAdminLogon	1= allow auto logon 0=disabled The value won't exist unless the user set up autologon.	Immediately	XP, V
Auto Logon Set - Password	SOFTWARE	SOFTWARE\Microsoft\Windows NT\CurrentVersion\ Winlogon / DefaultPassword	If autologon is set, the password must be present in this value in the clear	Immediately	XP, V
Class Identifiers	SOFTWARE	SOFTWARE\Classes\CLSID	Class identifier information, GUIDs on Applications and processes.	N/A	XP, V, 7
Group Memberships	SOFTWARE	SOFTWARE\Microsoft\Windows\CurrentVersion\Group Policy\GroupMembership	List of groups with which user is associated.	Immediately	XP, V, 7

Information	File	Location	Description	When Updated	Version
Home Group	SOFTWARE	SOFTWARE\Microsoft\Windows\ CurrentVersion\HomeGroup\ SharingPreferences\<sid>		N/A	7
ICQ Information	SOFTWARE	SOFTWARE\Mirabilis\ICQ\Owner	Stores the User Identification Number (UIN).	At logon	
Indexed Folders	SOFTWARE	SOFTWARE\Microsoft\Window Search\ CrawlScopeManager\ Windows\ SystemIndex\ WorkingSetRules\<#>	Reports the folders currently being indexed for the Search utility.	Upon adding a folder.	V, 7
Install Date	SOFTWARE	SOFTWARE\\Microsoft\Windows NT\ CurrentVersion	Lists the date the operating system was installed.	NA	XP, V, 7
Installed Application List	SOFTWARE	SOFTWARE\Microsoft\Windows\ CurrentVersion\ Uninstall	List of installed applications to use for uninstall.	N/A	XP, V, 7
Installed Application List	SOFTWARE	SOFTWARE\Wow6432Node\ <appname>	List of installed 32-bit applications.	N/A	7
Installed Application List	SOFTWARE	SOFTWARE\Wow6432Node\Microsoft\ Windows\CurrentVersion\ SharedDLLs	List of executables for installed applications.	N/A	7
Installed Application List	SOFTWARE	SOFTWARE\Microsoft\Windows\ CurrentVersion\ App Paths\<appname>	Installed list of applications	N/A	XP, V, 7
Installed Internet Browsers	SOFTWARE	SOFTWARE\Clients\StartMenuInternet \ <appname>	List of installed Internet browsers.	N/A	XP, V, 7

Information	File	Location	Description	When Updated	Version
Installed Internet Browsers - Default Browser	SOFTWARE	SOFTWARE\Clients\StartMenuInternet / default	Default installed Internet browser	N/A	
Last Logged on User	SOFTWARE	SOFTWARE\Microsoft\Windows\ CurrentVersion\Authentication\ LogonUI	Displays the user name of the last logged on user, computer name, and date/time of last logon in the key last modified date/time stamp. If the shutdown is normal, the subkey is modified to logoff time.	N/A	V, 7
Last User Logged In	SOFTWARE	SOFTWARE\\Microsoft\Windows NT\ CurrentVersion\Winlogon	Lists the last user that logged in to the system. This can be local or domain account.	NA	
Libraries	SOFTWARE	SOFTWARE\Microsoft\Windows Search\Gather\Windows\SystemIndex\ StartPages\<#>		Upon creation	7
Logon Banner Message	SOFTWARE	SOFTWARE\\Microsoft\Windows\ CurrentVersion\Policies\System\ LegalNoticeText	Contains the banner that appears at boot time. Users must click through the log-on banner to log on to a system.	NA	
Logon Banner Message	SOFTWARE	SOFTWARE\\Microsoft\Windows\ CurrentVersion\Policies\System\ LegalNoticeText	Contains user-defined data.	NA	
Logon Banner Title	SOFTWARE	SOFTWARE\\Microsoft\Windows\ CurrentVersion\Policies\System\ LegalNoticeCaption	Contains user-defined data.	NA	

Information	File	Location	Description	When Updated	Version
Logon Info—Default User and Domain Name	SOFTWARE	SOFTWARE\\Microsoft\Windows NT\CurrentVersion\Winlogon	Identifies the default user and the associated domain name.	NA	
Logon Info—Legal Notices on Bootup	SOFTWARE	SOFTWARE\\Microsoft\Windows NT\CurrentVersion\Winlogon	Contains legal notices that appear at boot time. Users must click through the log-on banner to log on to a system.	NA	
Network Cards	SOFTWARE	SOFTWARE\Microsoft\Windows NT\CurrentVersion\ NetworkCards\#	Lists installed network cards. The value can match up to the GUID stored in the SYSTEM file at SYSTEM\ControlSet###\Services\tcpip\Parameters\Interfaces\<guid>.	N/A	XP, V, 7
O\S Version	SOFTWARE	SOFTWARE\\Microsoft\Windows NT\CurrentVersion	Identifies the currently installed OS version and service pack release.	NA	XP, V, 7
Password Hint XP	SOFTWARE	SOFTWARE\Microsoft\Windows\CurrentVersion\Hints\<username>	XP Password hint storage location.	Immediately	XP
Passwords—Cached Logon Password Maximum	SOFTWARE	SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon	Control of max passwords stored in the cached passwords in SECURITY file.	N/A	XP
Printer Properties for Installed Printers	SOFTWARE	SOFTWARE\Microsoft\Windows NT\CurrentVersion\Print\Printers\<printername>	Detailed printer information, including user-entered properties from Control Panel.	N/A	XP, V, 7
Product ID	SOFTWARE	SOFTWARE\Microsoft\Windows NT\CurrentVersion	Lists the Windows OS product key.	NA	XP, V, 7

Information	File	Location	Description	When Updated	Version
Product Name	SOFTWARE	SOFTWARE\\Microsoft\Windows NT\ CurrentVersion	Lists the name of the operating system.	NA	XP, V, 7
Profile list	SOFTWARE	SOFTWARE\\Microsoft\Windows NT\ CurrentVersion\ProfileList	Contains the user security identifier for users with a profile on the system.	NA	XP, V, 7
ReadyBoost Attachments	SOFTWARE	SOFTWARE\Microsoft\Windows NT\ CurrentVersion\ EMDMgmt\<driveid>	List of attached USB devices for ReadyBoost utility.	N/A	V, 7
Recycle Bin Info - XP	SOFTWARE	SOFTWARE\Microsoft\Windows\ CurrentVersion\Explorer\BitBucket\ <driveletter>	Windows XP Recycler info by drive letter, Max Capacity in MB, NukeOnDelete 0=Bin being used (default) 1= Bin is being bypassed	N/A	XP
Registered Organization	SOFTWARE	SOFTWARE\\Microsoft\Windows NT\ CurrentVersion	Identifies the registered organization entered during installation. Note this information may be modified after installation.	NA	XP, V, 7
Registered Owner	SOFTWARE	SOFTWARE\\Microsoft\Windows NT\ CurrentVersion	Identifies the registered owner entered during installation. Note this information may be modified after installation.	NA	XP, V, 7
Restore Point Information	SOFTWARE	SOFTWARE\Microsoft\Windows NT\ CurrentVersion\ SystemRestore	System Restore parameters	N/A	XP
Restricted Access to Removable Media	SOFTWARE	SOFTWARE\\Microsoft\WindowsNT\ CurrentVersion\ Winlogon	Lists allocated CD-ROMS and floppies that are set to 0 (restricted).	NA	XP

Information	File	Location	Description	When Updated	Version
Run	SOFTWARE	SOFTWARE\Microsoft\Windows\ CurrentVersion\ Run	Lists programs that run automatically when the system boots.	NA	XP, V, 7
Startup Location	SOFTWARE	SOFTWARE\Microsoft\Command Processor / AutoRun	The AutoRun runs any application noted when cmd.exe is run.	N/A	
Startup Location	SOFTWARE	SOFTWARE\Microsoft\Windows NT\ CurrentVersion\Winlogon/Userinit	Applications to start on bootup.	N/A	
Startup Software	SOFTWARE	SOFTWARE\Microsoft\Windows\ CurrentVersion\Run	Stores the applications automatically launched at boot time. This key is a good place to look for trojans.	NA	XP, V, 7
Startup Software	SOFTWARE	SOFTWARE\\Microsoft\Windows\ CurrentVersion\ RunOnce	Stores the applications automatically launched at boot time. This key is a good place to look for trojans.	NA	XP, V, 7
System Restore Info	SOFTWARE	SOFTWARE\Microsoft\WindowsNT\ CurrentVersion\ SystemRestore	System Restore settings and info		V, 7
Time Synchronization with Internet - Servers	SOFTWARE	SOFTWARE\Microsoft\Windows\ CurrentVersion\ DateTime\Servers		N/A	XP, V, 7
Turn off UAC Behavior	SOFTWARE	SOFTWARE\Microsoft\Widows\ CurrentVersion\Policies\System\ *ConsentPromptBehaviorAdmin Value*	Turn off the prompts to Continue when running a program needing elevated rights. Turns off Cancel or Allow. 0 is off, 2 is on (Default)		V, 7

Information	File	Location	Description	When Updated	Version
UAC – On or Off	SOFTWARE	SOFTWARE\Microsoft\Windows\ CurrentVersion\Policies\System\ *EnableLUA_Value*	Identifies whether the UAC is on or off. By default it is on: value 1. If off: value 0		V, 7
USB ID linked to Volume Serial Number	SOFTWARE	SOFTWARE\Microsoft\WindowsNT\ CurrentVersion\EMDMgmt	Tracks USB keys by identifier and by volume serial number. Date and time if tested to be used as cache is stored along with USB size		V, 7
User Account Control	SOFTWARE	SOFTWARE\Microsoft\Windows\ CurrentVersion\Policies\System	UAC status 1=Enabled 0=Not Enabled	Upon changing	V, 7
User Name and SID	SOFTWARE	SOFTWARE\Microsoft\WindowsNT\ CurrentVersion\ ProfileList\ **Note:** See "User Name and SID" in *SAM Information* on page 19.	Contains the username and SID in hex. You must convert the last three hex numbers to decimal to determine the decimal version of the SID that is used in the Recycler and System Volume Information folder.	NA	XP, V, 7
WinZip Information	SOFTWARE	SOFTWARE\Nico Mak Computing	Contains WinZip information.		XP, V, 7
Wireless Vista, Windows 7	SOFTWARE	SOFTWARE\Microsoft\Windows NT\ CurrentVersion\ NetworkList\Profiles\ <guid>	Each GUID is a connection.	N/A	V, 7
Wireless Vista, Windows 7	SOFTWARE	SOFTWARE\Microsoft\Windows NT\ CurrentVersion\ NetworkList\ Signatures\Managed (or Unmanaged)\<guid>	Managed tracks hardwired connections, Unmanaged tracks wireless connections.	N/A	V, 7

Information	File	Location	Description	When Updated	Version
Wireless XP	SOFTWARE	SOFTWARE\Microsoft\WZCSVC\ Parameters\Interfaces\{0E271E68-9033-4A25-9883-A020B191B3C1} / Static#####	SSIDs are located in the Static# values followed by 4 digits.	Immediately	XP
Wireless XP	SOFTWARE	SOFTWARE\Microsoft\EAPOL\ Parameters\Interfaces\{0E271E68-9033-4A25-9883-A020B191B3C1} / #	SSIDs are located in the decimal number values.	N/A	XP

SYSTEM Information

Information	File	Location	Description	When Updated	Version
$MFT Zone Definition	SYSTEM	SYSTEM\ControlSet###\Control\ FileSystem / NtfsMftZoneReservation	Values 1-4: 1=12.5% 2=25% 3=37.5% 4=50% These values are defined according to Microsoft; however, values of 0 are common defaults and may be the same as a 1.	N/A	XP, V, 7
Automatic time zone adjustment	SYSTEM	SYSTEM\ControlSet###\Control\ TimeZoneInformation\ *DynamicDaylightTimeDisabled Value*	0 Default – On 1 Disabled		V, 7
Clearing Page File at Shutdown	SYSTEM	SYSTEM\ControlSet###\Control\ Session Manager\Memory Management / ClearPageFileAtShutdown	0=Off (default) 1=On	N/A	XP, V, 7

Information	File	Location	Description	When Updated	Version
Computer Name	SYSTEM	SYSTEM\ControlSet###\Control\ ComputerName\ComputerName	Identifies the computer's name defined in System Properties.	NA	XP, V, 7
Current Control Set	SYSTEM	SYSTEM\Select	Identifies which control set is current.	NA	XP, V, 7
Current Control Set	SYSTEM	SYSTEM\Select\Current	Contains information about the system's configuration settings.	NA	XP, V, 7
Display	SYSTEM	SYSTEM\ControlSet###\Enum\ Display	Monitor settings	N/A	XP, V, 7
DLLs Loaded at Bootup	SYSTEM	SYSTEM\ControlSet###\Control\ SessionManager\KnownDLLs	Listing of implicitly loaded DLL files at startup.		
Dynamic Disk	SYSTEM	SYSTEM\\ControlSetXXX\Services\ DMIO\Boot Info\Primary Disk Group	Identifies the most recent dynamic disk mounted in the system.	NA	XP, V, 7
Event Log Restrictions	SYSTEM	SYSTEM\ControlSet###\Services\ EventLog\ Application	Identifies who can read your event logs. A value of 1 restricts access; 0 permits access for guest and mull users.	NA	XP, V, 7
Event Logs	SYSTEM	SYSTEM\ControlSetXXX\Services\ Eventlog	Identifies the location of Event logs.	NA	XP, V, 7
Firewall Enabled	SYSTEM	SYSTEM\ControlSet###\Services\ SharedAccess\ Parameters\ FirewallPolicy\ StandardProfile / EnableProfile	0=Off 1=On (default)	Immediately	XP, V, 7
Floppy Disk Information	SYSTEM	SYSTEM\ControlSet###\Enum\FDC\ <device>	Floppy disk controller info.	N/A	XP, V, 7
Home Group	SYSTEM	SYSTEM\ControlSet###\services\ HomeGroupProvider\ServiceData		N/A	7

Information	File	Location	Description	When Updated	Version
Human Interface Devices	SYSTEM	SYSTEM\ControlSet###\Enum\HID	Includes keyboards, mice, trackballs, etc.	N/A	XP, V, 7
IDE Device Information	SYSTEM	SYSTEM\ControlSet###\Enum\IDE\ <device>	HDD, CD, DVD, and other attached hardware.	N/A	XP, V, 7
Last Accessed Date and Time setting	SYSTEM	SYSTEM\ControlSet###\Control\ FileSystem*NtfsDisableLastAccessUpdate Value*	0 On 1 Default - Disabled		XP, V, 7
LPT Device Information	SYSTEM	SYSTEM\ControlSet###\Enum\ LPTENUM\ <device>	Parallel printer information to LPT port.	N/A	XP, V, 7
Memory Saved During Crash	SYSTEM	SYSTEM\ControlSet###\Control\ CrashControl / DumpFile	Shows path to crash dump memory capture.	N/A	XP, V, 7
Memory Saved During Crash Enabled	SYSTEM	SYSTEM\ControlSet###\Control\ CrashControl / CrashDumpEnabled	0=None 1=Complete 2=Kernel Memory Dump 3=Small Memory Dump (64k)	N/A	XP, V, 7
Mounted Devices	SYSTEM	SYSTEM\MountedDevices	Lists current and prior mounted devices that use a drive letter.	Immediately	XP, V, 7
Mounted Devices	SYSTEM	SYSTEM\MountedDevices\	Change: Now using USB ID and not ParentIDPrefix		
Network Cards	SYSTEM	SYSTEM\ControlSet###\Services\ tcpip\Parameters\Interfaces\<guid>	GUID matches the network card GUIDs at Microsoft\Windows NT\ CurrentVersion\NetworkCards\#.	N/A	XP, V, 7
Number of Processors in System	SYSTEM	SYSTEM\ControlSet###\Control\ Session Manager\Environment / NUMBER_OF_PROCESSORS	The value stored in this value name is the number of processors on the system.	N/A	XP, V, 7

Information	File	Location	Description	When Updated	Version
Pagefile	SYSTEM	SYSTEM\ControlSetXXX\Control\ Session Manager\Memory Management	Contains the page file settings such as location, size, set to wipe, etc.	View updates immediately; however, not effective until reboot.	XP, V, 7
PCI Bus Device Information	SYSTEM	SYSTEM\ControlSet###\Enum\PCI	PCI bus device information	N/A	XP, V, 7
PDA Information	SYSTEM	SYSTEM\ControlSet###\Enum\USB	Contains PDA information.	NA	
Prefetch	SYSTEM	SYSTEM\ControlSet###\Control\ Session Manager\Memory Management\PrefetchParameters / EnablePrefetcher	0=Prefetch disabled 1=Applications Only 2=Boot Only 3=Application and Boot Prefetcher	N/A	XP, V, 7
Printer Information	SYSTEM	SYSTEM\ControlSet###\Control\Print \Environments\WindowsNTx86\ Drivers\Version…	Contains information about the current printer.	Immediately	XP, V, 7
Printers—Currently Defined	SYSTEM	SYSTEM\ControlSet###\Control\Print \Printers	Lists all printers that are configured on the current system.	Immediately	XP, V, 7
Remote Desktop	SYSTEM	SYSTEM\ControlSet###\Control\ Terminal Server / fDenyTSConnections	fDenyTSConnections=1 Remote Desktop Off fDenyTSConnections=0 Remote Desktop On	Immediately upon change	XP, V
SCSI Device Information	SYSTEM	SYSTEM\ControlSet###\Enum\SCSI	SCSI device settings; includes VHD device info.	N/A	XP, V, 7

Information	File	Location	Description	When Updated	Version
Serial Port Device Information	SYSTEM	SYSTEM\ControlSet###\Enum\ SERENUM	Serial port device settings	N/A	XP, V, 7
Services	SYSTEM	SYSTEM\ControlSet###\Services	List of services.	N/A	XP, V, 7
Shared Folders	SYSTEM	SYSTEM\ControlSet###\Services\ lanmanserver\ Shares / <shared folder name>	List of shared folders on system.	Immediately	XP
Shutdown Time	SYSTEM	SYSTEM\ControlSetXXX\Control\ Windows	Lists the system shutdown time.	NA	XP, V, 7 **Note:** Removed in Vista first release and returned in service pack
Startup Location	SYSTEM	SYSTEM\ControlSet###\Control\ SessionManager\BootExecute	Software startup location. **Note:** This has not been tested in Windows 7	N/A	XP, V, 7
Storage - Volumes and Removable Media	SYSTEM	SYSTEM\ControlSet###\Control\ Enum\Volume\<guid>	Stores information on storage media, including beginning volume offset and size.	Immediately	XP, V, 7
Storage - Volumes and Removable Media	SYSTEM	SYSTEM\ControlSet###\Control\ Enum\ RemovableMedia\<guid>	Stores information on removable media.	Immediately	XP, V, 7
Storage Device Information	SYSTEM	SYSTEM\ControlSet###\Enum\ STORAGE	HDD info including partition sizes	N/A	XP, V, 7

Information	File	Location	Description	When Updated	Version
TCP\IP data	SYSTEM	SYSTEM\ControlSetXXX\Services\ TCPIP\ Parameters	Lists the current system's domain and hostname data.	NA	XP, V, 7
TCP\IP Settings of a Network Adapter	SYSTEM	SYSTEM\ControlSetXXX\Services\ *adapter*\ Parameters\TCPIP	Lists the current system's IP address and gateway information.	Immediately	XP, V, 7
Time Synchronization with Internet - Enabled	SYSTEM	SYSTEM\ControlSet###\Services\ W32Time\ Parameters / Type	NoSynch=Disabled NTP=Enabled	Immediately	XP, V, 7
Time Synchronization with Internet - Type	SYSTEM	SYSTEM\ControlSet###\Services\ W32Time\ Parameters / NtpServer	Shows current time provider (or if disabled, the last time provider) - NTP is time.windows.com (default - Microsoft) or time.nist.gov	Immediately	XP, V, 7
Time Zone	SYSTEM	SYSTEM\ControlSet001(or002)\ Control\TimeZoneInformation\ StandardName	Identifies the time zone entered during installation. Note this information may be modified after installation.	Immediately	XP, V, 7
USB Devices	SYSTEM	SYSTEM\Enum\USBSTOR	Lists the system's USB devices.	Immediately	XP, V, 7
USB Tracking	SYSTEM	SYSTEM\ControlSet###\Enum\ USBSTOR	Change: Now using USB ID and not ParentIDPrefix		V, 7
Write Block USB Devices	SYSTEM	SYSTEM\ControlSet###\Control\ torageDevicePolicies / Write Protect	0=Disabled 1=Enabled **Note:** This began with Windows XP Service Pack 2.	N/A	XP SP2, V, 7