

ACCESSDATA SUPPLEMENTAL APPENDIX

Registry Quick Find Chart

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

- *Vista Registry Keys and Values* on page 2
- *AOL Instant Messenger* on page 3
- *ICQ* on page 4
- *Internet Explorer* on page 4
- *MSN Messenger* on page 5
- *Outlook and Outlook Express* on page 6
- *Windows Messenger* on page 6
- *Yahoo! Messenger* on page 7
- *System Information* on page 8
- *Networking* on page 10
- *User Data* on page 11
- *User Application Data* on page 14

VISTA REGISTRY KEYS AND VALUES

Information	File	Location	Description	When Updated
IntelliForms	NTUSER.DAT	Software\Microsoft\Internet Explorer\IntelliForms	Encrypted user data in Storage1 and Storage2 (old PSSP info)	
Password Hint	SAM	Domains\Account\Users\<RID>\F_Value\UserPasswordHint	Shows a logon password hint if initiated by the user	
UAC – On or Off	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	
System Restore Info	SOFTWARE	Microsoft\WindowsNT\CurrentVersion\SystemRestore	System Restore settings and info	
Turn off UAC Behavior	SOFTWARE	Microsoft\Windows\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)	
USB ID linked to Volume Serial Number	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	
Automatic time zone adjustment	SYSTEM	ControlSet###\Control\TimeZoneInformation\DynamicDaylightTimeDisabled Value	0 Default – On 1 Disabled	
Last Accessed Date and Time setting	SYSTEM	ControlSet###\Control\FileSystem\NtfsDisableLastAccessUpdate Value	0 On 1 Default - Disabled	
USB Tracking	SYSTEM	ControlSet###\Enum\USBSTOR	Change: Now using USB ID and not ParentIDPrefix	
Mounted Devices	SYSTEM	MountedDevices\	Change: Now using USB ID and not ParentIDPrefix	

AOL INSTANT MESSENGER

Information	File	Location	Description	When Updated
Away Messages	NTUSER.DAT	\Software\America Online\ AOL Instant Messenger(TM)\ CurrentVersion\Users\screen name\IAMGoneList	Shows default and customized Away messages.	Immediately
File Transfers & Sharing	NTUSER.DAT	\Software\America Online\ AOL Instant Messenger(TM)\ CurrentVersion\Users\screen name\Xfer	Shows settings for file transfers and sharing.	Immediately
Last User	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
Profile Info	NTUSER.DAT	\Software\America Online\ AOL Instant Messenger(TM)\ CurrentVersion\Users\screen name\ DirEntry	Shows user profile information (optional).	Immediately
Recent Contacts	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.
Registered Users	NTUSER.DAT	\Software\America Online\ AOL Instant Messenger (TM)\ CurrentVersion\Users	Shows registered AIM users on the machine.	At sign-on
Saved Buddy List	NTUSER.DAT	\Software\America Online\ AOL Instant Messenger(TM)\ CurrentVersion\Users\username\ ConfigTransport	Shows the directory path of a saved Buddy List, a BLT file.	Immediately

ICQ

Information	File	Location	Description	When Updated
ICQ	NTUSER.DAT	\Software\Mirabilis\ICQ*	Lists IM contacts, file transfer information, etc.	Not applicable
ICQ Information	SOFTWARE	\Software\Mirabilis\ICQ\Owner	Stores the User Identification Number (UIN).	At logon
Last User	NTUSER.DAT	\Software\Mirabilis\ICQ\Owners - LastOwner	Shows the last logged-in user.	At logon
Nickname	NTUSER.DAT	\Software\Mirabilis\ICQ\Owners\UIN - Name	Nickname of user (optional value).	At logon
Registered Users	NTUSER.DAT	\Software\Mirabilis\ICQ\Owners\UIN	UIN folder is named for the user.	At logon

INTERNET EXPLORER

Information	File	Location	Description	When Updated
IE Auto Logon and password	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
IE Search Terms	NTUSER.DAT	\Software\Microsoft\Protected Storage System Provider\SID\Internet Explorer\Internet Explorer - q:StringIndex	Stores IE search terms with date and time stamp.	Immediately
IE Settings	NTUSER.DAT	\Software\Microsoft\Internet Explorer\Main	Stores IE settings such as start page, save directory, home page, and download location.	Immediately
IE URL History — Days Saved	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

Information	File	Location	Description	When Updated
Typed URLs	NTUSER.DAT	\Software\Microsoft\Internet Explorer\Typed URLs	Stores data entered into the URL Address Bar.	When the application closes
Web Form Data	NTUSER.DAT	\Software\Microsoft\Protected Storage System Provider\SID\Internet Explorer\Internet Explorer - q:StringIndex	Stores form data provided within IE.	Immediately
IE Auto-Complete Passwords	NTUSER.DAT	\Software\Microsoft\Internet Explorer\IntelliForms	Stores web page auto-complete passwords. These are encrypted values.	Immediately
IE Auto-Complete Web Addresses	NTUSER.DAT	\Software\Microsoft\Protected Storage System Provider	Lists web pages wherein autocomplete was utilized.	Immediately
IE Default Download Directory	NTUSER.DAT	\Software\Microsoft\Internet Explorer	Identifies the default download directory when utilizing Internet Explorer.	Immediately

MSN MESSENGER

Information	File	Location	Description	When Updated
MSN Messenger	NTUSER.DAT	\Software\Microsoft\MessengerService\ListCache\NET MessengerService*	Contains IM groups, contacts, file transfer information, etc. for MSN Messenger.	Most on signoff; however, FTReceive is immediate.
File Sharing	NTUSER.DAT	\Software\Microsoft\MSNMessenger\FileSharing - Autoshare	Shows if file sharing is turned on.	Immediately
File Transfers	NTUSER.DAT	\Software\Microsoft\MSNMessenger\ - FTReceiveFolder	Shows the location of the Received Files folder.	Immediately
Logging Enabled	NTUSER.DAT	\Software\Microsoft\MSNMessenger\PerPass portSettings\#####\ - MessageLoggingEnabled	Shown if message logging is turned on.	Immediately

Information	File	Location	Description	When Updated
Message History	NTUSER.DAT	\Software\Microsoft\MSN Messenger\PerPass portSettings\#####\- MessageLog Path	Shows the location of message history files.	Immediately
Saved Contact List	NTUSER.DAT	\Software\Microsoft\Messenger Service - ContactListPath	Shows the location of a saved Contact List (CTT) file.	Immediately

OUTLOOK AND OUTLOOK EXPRESS

Information	File	Location	Description	When Updated
Account Passwords	NTUSER.DAT	\Software\Microsoft\Protected Storage SystemProvider\SID\Identification\INETCOMM Server Passwords	Stores Outlook and Outlook Express account passwords.	Immediately
Outlook Temporary Attachment Directory	NTUSER.DAT	\Software\Microsoft\Office\version\Outlook\Security	Identifies the location where attachments are stored when they are opened from Outlook.	Immediately

WINDOWS MESSENGER

Information	File	Location	Description	When Updated
Contact List	NTUSER.DAT	\Software\Microsoft\MessengerService>ListCache\ .NET Messenger Service	Contains Contact, Allow, Block, and Reverse entries.	At sign-off
File Transfers	NTUSER.DAT	\Software\Microsoft\Messenger Service - FtReceiveFolder	Shows the location of the Received Files folder.	Immediately
Last User	NTUSER.DAT	\Software\Microsoft\MessengerService>ListCache\ .NET Messenger Service - IdentityName	Screen name of last logged-in user.	At sign-off

YAHOO! MESSENGER

Information	File	Location	Description	When Updated
Chat Rooms	NTUSER.DAT	\Software\Yahoo\Pager\profiles\ <i>screen name</i> \Chat	Shows information for chat rooms visited or created.	Immediately
File Transfers	NTUSER.DAT	\Software\Yahoo\Pager\ File Transfer (global value)	Shows number of transfers in and out.	Immediately
File Transfers	NTUSER.DAT	Software\Yahoo\Pager\profiles\ <i>screen name</i> \File Transfer (user specific)	Shows settings for file transfers.	Immediately
Identities	NTUSER.DAT	\Software\Yahoo\Pager\profiles\ screen name - All Identities, Selected Identities	Shows alternate user identities.	Unknown
IMVs MRU list	NTUSER.DAT	Software\Yahoo\Pager\profiles\ screen name\IMVironments (user-specific value)	Shows usage of IMVironments.	Immediately
IMV Usage	NTUSER.DAT	\Software\Yahoo\Pager\ IMVironments (global value)	Shows usage of IMVironments.	Immediately
Last User	NTUSER.DAT	\Software\Yahoo\ Pager - Yahoo! User ID	Last logged-in user.	Immediately
Message Archiving	NTUSER.DAT	\Software\Yahoo\Pager\profiles\ <i>screen name</i> \Archive	Shows settings for message archiving.	Immediately
Password	NTUSER.DAT	\Software\Yahoo\ Pager - EOptions string	Encrypted password.	Immediately
Recent Contacts	NTUSER.DAT	Software\Yahoo\Pager\profiles\ screen name\IMVironments\Recent	Shows recent contacts and which IMV was used.	Immediately
Saved Password	NTUSER.DAT	\Software\Yahoo\ Pager - Save Password	Shows if the password is saved.	Immediately
Screen Names	NTUSER.DAT	\Software\Yahoo\Pager\profiles\ <i>screen name</i>	Shows registered screen names and identities.	Immediately
Yserver	NTUSER.DAT	\Software\Yahoo\Yserver	Points to a directory location for file transfer information.	Not applicable

SYSTEM INFORMATION

Information	File	Location	Description	When Updated
Computer Name	SYSTEM	\ControlSet###\Control\ComputerName\ComputerName	Identifies the computer's name defined in System Properties.	Not applicable
Current Control Set	SYSTEM	\Select	Identifies which control set is current.	Not applicable
Current Control Set	SYSTEM	\Select\Current	Contains information about the system's configuration settings.	Not applicable
Dynamic Disk	SYSTEM	\ControlSetXXX\Services\DMIO\Boot Info\Primary Disk Group	Identifies the most recent dynamic disk mounted in the system.	Not applicable
Event Logs	SYSTEM	\ControlSetXXX\Services\Eventlog	Identifies the location of Event logs.	Not applicable
Install Date	SOFTWARE	\Microsoft\Windows NT\CurrentVersion	Lists the date the operating system was installed.	Not applicable
Last User Logged In	SOFTWARE	\Microsoft\Windows NT\CurrentVersion\Winlogon	Lists the last user that logged in to the system. This can be local or domain account.	Not applicable
Logon Banner Message	SOFTWARE	\Microsoft\Windows\CurrentVersion\Policies\System\LegalNoticeText	Contains the banner that appears at boot time. Users must click through the logon banner to log on to a system.	Not applicable
Logon Banner Message	SOFTWARE	\Microsoft\Windows\CurrentVersion\Policies\System\LegalNoticeText	Contains user-defined data.	Not applicable
Logon Banner Title	SOFTWARE	\Microsoft\Windows\CurrentVersion\Policies\System\LegalNoticeCaption	Contains user-defined data.	Not applicable

Information	File	Location	Description	When Updated
Logon Info—Default User and Domain Name	SOFTWARE	\Microsoft\Windows NT\CurrentVersion\Winlogon	Identifies the default user and the associated domain name.	Not applicable
Logon Info—Legal Notices on Bootup	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.	Not applicable
Mounted Devices	SYSTEM	\MountedDevices	Lists current and prior mounted devices that use a drive letter.	Immediately
OS Version	SOFTWARE	\Microsoft\Windows NT\CurrentVersion	Identifies the currently installed OS version and service pack release.	Not applicable
Pagefile	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.
PDA Information	SYSTEM	\ControlSet###\Enum\USB	Contains PDA information.	Not applicable
Product ID	SOFTWARE	\Microsoft\Windows NT\CurrentVersion	Lists the Windows OS product key.	Not applicable
Product Name	SOFTWARE	\Microsoft\Windows NT\CurrentVersion	Lists the name of the operating system.	Not applicable
Registered Organization	SOFTWARE	\Microsoft\Windows NT\CurrentVersion	Identifies the registered organization entered during installation. Note this information may be modified after installation.	Not applicable

Information	File	Location	Description	When Updated
Registered Owner	SOFTWARE	\Microsoft\Windows NT\CurrentVersion	Identifies the registered owner entered during installation. Note this information may be modified after installation.	Not applicable
Restricted Access to Removable Media	SOFTWARE	\Microsoft\WindowsNT\CurrentVersion\Winlogon	Lists allocated CD-ROMS and floppies that are set to 0 (restricted).	Not applicable
Run	SOFTWARE	\Microsoft\Windows\CurrentVersion\Run	Lists programs that run automatically when the system boots.	Not applicable
Shutdown Time	SYSTEM	\ControlSetXXX\Control\Windows	Lists the system shutdown time.	Not applicable
Time Zone	SYSTEM	\ControlSet001 (or 002)\Control\TimeZoneInformation\StandardName	Identifies the time zone entered during installation. Note this information may be modified after installation.	Immediately
USB Devices	SYSTEM	\Enum\USBSTOR	Lists the system's USB devices.	Immediately

NETWORKING

Information	File	Location	Description	When Updated
Local Groups	SAM	\Domains\Builtin\Aliases\Names	Lists local account security identifiers.	Not applicable
Local Users	SAM	\Domains\Account\Users\Names	Lists local account security identifiers.	Not applicable
Map Network Drive MRU	NTUSER.DAT	\Software\Microsoft\Windows\CurrentVersion\Explorer\Map Network Drive MRU	Contains a most recently used list of mapped network drives.	Not applicable
Printers—Currently Defined	SYSTEM	\ControlSet###\Control\Print\Printers	Lists all printers that are configured on the current system.	Immediately

Information	File	Location	Description	When Updated
Printer— Default	NTUSER.DAT	\Software\Microsoft\WindowsNT\CurrentVersion\Windows	Identifies the current default printer.	Immediately
	NTUSER.DAT	\printers	Identifies the current default printer.	On shutdown
Printer Information	SYSTEM	\ControlSet###\Control\Print\Environments\WindowsNTx86\Drivers\Version...	Contains information about the current printer.	Immediately
Profile list	SOFTWARE	\Microsoft\Windows NT\CurrentVersion\ProfileList	Contains the user security identifier for users with a profile on the system.	Not applicable
TCP/IP data	SYSTEM	\ControlSetXXX\Services\TCPIP\Parameters	Lists the current system's domain and hostname data.	Not applicable
TCP/IP Settings of a Network Adapter	SYSTEM	\ControlSetXXX\Services\adapter\Parameters\TCPIP	Lists the current system's IP address and gateway information.	Immediately

USER DATA

Information	File	Location	Description	When Updated
EFS	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.	Not applicable

Information	File	Location	Description	When Updated
Event Log Restrictions	SYSTEM	\ControlSet###\Services\EventLog\Application	Identifies who can read your event logs. A value of 1 restricts access; 0 permits access for guest and null users.	Not applicable
	SECURITY	\ControlSet###\Services\EventLog\Application	Identifies who can read your event logs. A value of 1 restricts access; 0 permits access for guest and null users.	Not applicable
File Extensions\Program Association	NTUSER.DAT	\Software\Microsoft\Windows\CurrentVersion\Explorer\FileExts	Identifies associated programs with file extensions.	Immediately
Last Logon Time	SAM	\SAM\Domains\Account\Users\F Key	Bytes 9–16 store the last log-on time.	Not applicable
Last Time Password Changed	SAM	\SAM\Domains\Account\Users\F Key	Bytes 25–32 store the last time the password was changed.	Not applicable
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.	Not applicable
Last Failed Login	SAM	\SAM\Domains\Account\Users\F Key	Bytes 41-48 store the last unsuccessful logon.	Not applicable
MRU—Last Visited	NTUSER.DAT	\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\	Lists the application and filename of the most recent files opened in Windows.	Immediately
MRU—Open Saved	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

Information	File	Location	Description	When Updated
MRU—Recent Documents	NTUSER.DAT	\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\	Identifies the documents in the Recent Documents list available from the Windows Start menu.	Immediately
MRU—Run MRU	NTUSER.DAT	\Software\Microsoft\Windows\CurrentVersion\Explorer\RunMRU	Lists the most recent commands entered in the Windows Run box.	Immediately
POP3 Passwords	NTUSER.DAT	\Software\Microsoft\Internet Account Manager\Accounts\0000000#	Stores the user's POP3 passwords. # is a digit identifying that particular account.	Immediately
Run	NTUSER.DAT	\Software\Microsoft\Windows\CurrentVersion\Run	Lists programs that run automatically when the user logs on.	Not applicable
Screen Savers and wallpaper	NTUSER.DAT	\Control Panel\Desktop\	Identifies the system's screen saver and wallpaper.	Immediately
Theme—Current Theme	NTUSER.DAT	\Software\Microsoft\Windows\CurrentVersion\Themes	Identifies the Desktop theme and wallpaper.	Unknown
Theme—Last Theme	NTUSER.DAT	\Software\Microsoft\Windows\CurrentVersion\Themes\Last Theme	Identifies the Desktop theme and wallpaper.	Immediately
Converted Wallpaper	NTUSER.DAT	\Control Panel\Desktop	Identifies graphics that are converted to wallpaper.	Immediately
Converted Wallpaper	NTUSER.DAT	\Control Panel\Desktop	Identifies date and time of converted wallpaper.	Immediately

Information	File	Location	Description	When Updated
User Name and SID	SAM	\SAM\Domains\Account\Users\ V Key	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.	Not applicable
	SOFTWARE	\Microsoft\WindowsNT\CurrentVersion\ProfileList\	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.	Not applicable

USER APPLICATION DATA

Information	File	Location	Description	When Updated
Adobe	NTUSER.DAT	\Software\Adobe*	Lists Adobe products such as Acrobat* and FrameMaker*.	
AIM	NTUSER.DAT	\Software\America Online\AOL InstantMessenger\CurrentVersion\ Users\ <i>username</i>	Lists IM contacts, file transfer information, etc.	Immediately
Google Client History	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

Information	File	Location	Description	When Updated
Individual Application Information	NTUSER.DAT	\Software\%Application Name%	This class of registry keys contains the information each application stores in the registry.	Not applicable
Kazaa	NTUSER.DAT	\Software\Kazaa*	Stores configuration, search, download, IM data, etc. for Kazaa.	Not applicable
Media Player Recent List	NTUSER.DAT	\Software\Microsoft\MediaPlayer\Player\RecentFileList	Contains the user's most recently used list for Windows Media Player.	Immediately
Startup Software	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.	Not applicable
	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.	Not applicable
	SOFTWARE	\Microsoft\Windows\CurrentVersion\Run	Stores the applications automatically launched at boot time. This key is a good place to look for trojans.	Not applicable
	SOFTWARE	\Microsoft\Windows\CurrentVersion\RunOnce	Stores the applications automatically launched at boot time. This key is a good place to look for trojans.	Not applicable

Information	File	Location	Description	When Updated
WinZip Information	NTUSER.DAT	\Software\Nico Mak Computing\FileMenu	Stores the list of files extracted from WinZip archives.	Immediately
	SOFTWARE	\Nico Mak Computing	Contains WinZip information.	
Word—Recent Docs	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
Word—User Info	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
Access—Recent Databases	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
Excel—Recent Spreadsheets	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
Outlook—Recent Attachments	NTUSER.DAT	\Software\Microsoft\office\version\Common\Open Find\Microsoft Office Outlook\Settings\Save Attachment\File Name MRU	Microsoft Outlook recent documents.	Immediately
PowerPoint—Recent PPTs	NTUSER.DAT	\Software\Microsoft\office\version\Common\Open Find\Microsoft Office PowerPoint\Settings\Save As\File Name MRU	Microsoft PowerPoint recent documents.	Unknown
Publisher—Recent Documents	NTUSER.DAT	\Software\Microsoft\office\version\Common\Open Find\Microsoft Office Publisher\Settings\Save As\File Name MRU	Microsoft Publisher recent documents.	Unknown
Yahoo	NTUSER.DAT	\Software\Yahoo\Pager\Profiles*	Stores IM contacts, file transfer information, etc. for Yahoo!.	Not applicable

Information	File	Location	Description	When Updated
File Extension Associations	NTUSER.DAT	\Software\Microsoft\Windows\CurrentVersion\Explorer\FileExts\ <i>.EXT Type</i>	Lists file extension associations and files that have been opened with the Open With command.	Immediately
User Assist	NTUSER.DAT	\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist	Windows history logged with path and time stamp information.	Not applicable
ShellBags	NTUSER.DAT	\Software\Microsoft\Windows\Shell\BagMRU	Pointers to link history and other file and folder information.	Not applicable