THE RCFL PROGRAM'S
CONTINUING
EDUCATION
SERIES

NATIONAL PROGRAM OFFICE RCFL

WINDOWS VISTA FORENSIC QUICK START

FACT SHEET

Microsoft released Vista in early 2007, and it is already being encountered by forensic examiners. The purpose of this fact sheet is to provide a ‘Quick Start’ guide to acclimate the unfamiliar examiner to some of the differences between Vista and previous operating systems.

VISTA'S VERSIONS

Vista is available in five versions: Home Basic, Home Premium, Business, Ultimate and Enterprise. A matrix detailing the differences between the versions can be found at http://www.microsoft.com/windows/products/windowsvista/editions/choose.mspx. From a forensic perspective, it is important to note that Bitlocker Drive Encryption, Microsoft’s full volume encryption solution, is only available in the Ultimate and Enterprise editions. Additionally, the Encrypting File System (EFS) is available in the Business, Ultimate and Enterprise editions.

VISTA'S FILE SYSTEM

As with Windows XP, Vista continues to use NTFS for its file system. The WinFS file system, at one time rumored to be a part of Vista, has not been implemented.

While the directory structure utilized by Vista is similar to that of XP, a number of folders typically reviewed by examiners are now in different locations. Vista makes use of reparse points[1] to point legacy folders (such as \Documents and Settings) to Vista’s new file locations.

[1] A reparse point is a file system object that points to another location. The type of reparse point that provides for a folder to point to another folder is known as a junction.

XP/Vista File Path Comparison

Windows XP	Vista
\Documents and Settings*	\Users
\Documents and Settings\<user>	\Users\<user>
\Documents and Settings\<user>\Local Settings*	\Users\<user>\AppData\Local
\Documents and Settings\Recent*	\Users\<user>\AppData\Roaming\Microsoft\Windows\Recent
\Documents and Settings\Start Menu*	\Users\<user>\AppData\Roaming\Microsoft\Windows\Start Menu
\Documents and Settings\Local Settings\History	\Users\<user>\AppData\Local\Microsoft\Windows\History
\Documents and Settings\Local Settings\Temporary Internet Files	\Users\<user>\AppData\Local\Microsoft\Windows\Temporary Internet Files
\Documents and Settings\<user>\Application Data*	\Users\<user>\AppData
\Documents and Settings\<user>\Cookies*	\Users\<user>\AppData\Roaming\Microsoft\Windows\Cookies\Low
thumbs.db	\Users\<user>\AppData\Local\Microsoft\Windows\Explorer
\Recycled or \Recycler	\$Recycle.Bin

* Denotes a Vista reparse point

Certain user home directory folders have been renamed:

My Documents ---> Documents
My Pictures ---> Pictures
My Music ---> Music

A user's home directory now contains additional folders that were not present with XP—

- Downloads – The default download location
- Contacts – User's contacts
- Links – Windows Explorer favorites
- Saved Games – User's saved games
- Searches – Saved searches.

The Recycle Bin

Vista's recycle bin functionality differs drastically from that of XP. The \Recycled or \Recycler folders have been replaced with \$Recycle.Bin at the root of the volume. The INFO2 file, which XP used to track files moving in and out of the recycle bin, is no longer used. In its place are pairs of files. When a file is moved to the recycle bin, it is renamed with a random file name starting with $R, with its extension unchanged from the original deleted file. Accompanying this file is an administrative file with the same random file name and extension, starting with $I. This file contains the information which Vista uses to store the deleted files original name and location.

Disk Defragmentation

By default, Vista will run its disk defragmenter once per week. Obviously, disk defragmentation significantly impacts the ability to recover deleted files.

Internet Explorer Temporary Internet Files

Vista has adopted a new security model that implements restrictions on locations that applications can write to. This model results in Internet Explorer storing temporary Internet files in two locations:

\Users\<user>\AppData\Local\Microsoft\Windows\History\History.IE5

\Users\<user>\AppData\Local\Microsoft\Windows\History\Low\History.IE5

Files written as a result of browsing the Internet are maintained in the '\Low\History.IE5 folder. The other folder appears to be used for storage of files related to browsing within the local machine.

Cookies

The cookies directory structure schema is similar to that of Temporary Internet Files:

\Users\<user>\AppData\Roaming\Microsoft\Windows\Cookies and Low folders

\Users\<user>\AppData\Roaming\Microsoft\Windows\Cookies\Low

Link (.lnk) Files

The link file concepts appears to be largely unchanged between Vista and XP. Link files can be found at:

\Users\<user>\AppData\Roaming\Microsoft\Windows\Recent

Printer Spool

The creation of printer spool files appears similar between XP and Vista. Both the container spool file (.SPL) and the administrative file (.SHD) continue to be generated.

\Windows\System32\spool\printers

Thumbs Databases

Vista provides the ability to view thumbnails in four sizes. A separate thumbs database is created for each of these sizes and stored in a user's folder:

\User\<user>\AppData\Local\Microsoft\Windows\Explorer

The files are no longer stored in the directories containing the files viewed, as they were in XP.

Shadow Copy

Shadow Copy is a Vista feature that, according to Microsoft, is available in the Business, Ultimate and Enterprise additions. It allows a user to revert to previous versions of a file. Shadow copy appears to be essentially what was known under XP as System Restore, with expanded capability. Only changed blocks of data are stored, not the entire file, which may make data recovery more difficult.

Encrypting File System (EFS)

Vista continues to make EFS functionality available. According to Microsoft, it is available in the Business, Ultimate and Enterprise editions.

Bitlocker

Bitlocker is Vista's implementation of full volume encryption. It is available in the Ultimate and Enterprise editions. A partition that has been protected by Bitlocker can be identified by the string "FVE-FS" at the beginning of the partition.

A partition protected by Bitlocker can be decrypted if the Drive Encryption Key is available. The key may be stored on a removable piece of media such as a USB device, which can be inserted at boot time to provide authentication. The key can also be stored in a .txt or .bek file, a backup key file. The examination computer used to do the decryption must be running either the Ultimate or Enterprise version of Vista.

If a live machine with a Bitlocker protected volume is encountered, and the examiner has access to the machine, the key can be copied out through the Bitlocker Applet in the Control Panel. Additionally, the live machine can be imaged logically.

For More Information

To learn more about the RCFL Program, contact the National Program Office:

RCFL National Program Office

SSA Bryan Tepper, Unit Chief
Central Number:
703-985-3677
Email: npo@rcfl.gov

Mailing Address—

Engineering Research Facility
Building 27958-A
Quantico, VA 22135
Attn: ERF Annex
RCFL National Program Office

Web Site Address—

www.rcfl.gov