SWGDE Technical Notes on Microsoft Windows 7

Disclaimer:
As a condition to the use of this document and the information contained therein, the SWGDE requests notification by e-mail before or contemporaneous to the introduction of this document, or any portion thereof, as a marked exhibit offered for or moved into evidence in any judicial, administrative, legislative or adjudicatory hearing or other proceeding (including discovery proceedings) in the United States or any Foreign country. Such notification shall include: 1) The formal name of the proceeding, including docket number or similar identifier; 2) the name and location of the body conducting the hearing or proceeding; 3) subsequent to the use of this document in a formal proceeding please notify SWGDE as to its use and outcome; 4) the name, mailing address (if available) and contact information of the party offering or moving the document into evidence. Notifications should be sent to secretary@swgde.org.

It is the reader's responsibility to ensure they have the most current version of this document. It is recommended that previous versions be archived.

Redistribution Policy:
SWGDE grants permission for redistribution and use of all publicly posted documents created by SWGDE, provided that the following conditions are met:

1. Redistribution of documents or parts of documents must retain the SWGDE cover page containing the disclaimer.
2. Neither the name of SWGDE nor the names of contributors may be used to endorse or promote products derived from its documents.
3. Any reference or quote from a SWGDE document must include the version number (or create date) of the document and mention if the document is in a draft status.

Requests for Modification:
SWGDE encourages stakeholder participation in the preparation of documents. Suggestions for modifications are welcome and must be forwarded to the Secretary in writing at secretary@swgde.org. The following information is required as a part of the response:

a) Submitter's name
b) Affiliation (agency/organization)
c) Address
d) Telephone number and email address
e) Document title and version number
f) Change from (note document section number)
g) Change to (provide suggested text where appropriate; comments not including suggested text will not be considered)
h) Basis for change

Intellectual Property:
Unauthorized use of the SWGDE logo or documents without written permission from SWGDE is a violation of our intellectual property rights.

Individuals may not misstate and/or over represent duties and responsibilities of SWGDE work. This includes claiming oneself as a contributing member without actively participating in SWGDE meetings; claiming oneself as an officer of SWGDE without serving as such; claiming sole authorship of a document; use the SWGDE logo on any material and/or curriculum vitae.

Any mention of specific products within SWGDE documents is for informational purposes only; it does not imply a recommendation or endorsement by SWGDE.

Table of Contents

Table of Figures

Table of Tables

1. Scope

The scope of this document is to identify differences between current Microsoft operating systems (Windows Vista and XP) and the new Microsoft Windows® 7 as it applies to digital forensics, software and hardware tools. This document will start with an overview of the new Windows 7 software and then follow with the forensic implications following the typical forensic processing methods.

2. Overview of Windows 7

2.1 Versions

Windows 7 has six "flavors," ranging from basic to loaded, respectively:

1. Windows 7 Starter;
2. Windows 7 Home Basic;
3. Windows 7 Home Premium;
4. Windows 7 Business;
5. Windows 7 Enterprise; and
6. Windows 7 Ultimate.

With the exception of Windows 7 Starter, all of these operating systems are offered in both 32-bit and 64-bit. The 32-bit systems support a maximum of 4GB of RAM, and the 64-bit systems support a maximum of 192GB. Windows 7 remains substantially similar to Windows Vista. Windows 7 adds a variety of new features. The "Classic View" is no longer available in Windows 7.

2.1.1 Windows 7 Starter

This bare-bones program is offered in emerging markets only and will not be available in the United States. It only comes preinstalled on new hardware and includes internet browsing, communication, media technologies, photo manipulation, and parental controls.

2.1.2 Windows 7 Basic

This is the successor to Windows Vista Home. Microsoft states that it is meant for the home or a small business network. It contains Internet Explorer 8, Windows Media Center, Windows Movie Maker, and Windows Mail (the successor to Outlook). Automated indexing of the contents of the hard disk allows users to utilize instant searching. Windows 7 Basic supports 8 GB maximum physical memory in the 64-bit version.

2.1.3 Windows 7 Home Premium

This is the successor to Windows Vista Media Center, and it is what most retail OEMs are installed with. It incorporates all of the options available in Home Basic. In addition, it offers the aero glass interface, Windows Media Center, and HomeGroup Networking. It includes touch screen controls. Windows 7 Home Premium supports 16 GB maximum physical memory in the 64-bit version.

2.1.4 Windows 7 Professional

This edition is targeted towards enthusiasts and small business users. It includes all the features of Windows 7 Home Premium, and adds the ability to participate in a Windows Server domain. Additional features include operating as a Remote Desktop server, location aware printing, Encrypting File System, Presentation Mode, Backup and Restore Center Software Restriction Policies (but not the extra management features of AppLocker) and Windows XP Mode. Windows 7 Professional supports 192 GB maximum physical memory in the 64-bit version.

2.1.5 Windows 7 Enterprise

This program is available only to corporations or institutions that have volume licensing through Microsoft; it will not be available in retail markets. It basically incorporates all of the options found in Windows 7 Professional and adds BitLocker full volume encryption. Windows 7 Enterprise adds AppLocker Management features, Multilingual User Interface Pack, and Virtual Hard Disk Booting. It also adds a Subsystem for Unix-based Applications.

2.1.6 Windows 7 Ultimate

Windows 7 Ultimate contains the same features as Windows 7 Enterprise, but unlike the Enterprise edition, it is available to home users on an individual license basis. Windows 7 Home Premium and Windows 7 Professional users are able to upgrade to Windows 7 Ultimate for a fee using Windows Anytime Upgrade if they wish to do so. Unlike Windows Vista Ultimate, the Windows 7 Ultimate edition does not include the Windows Ultimate Extras feature or any exclusive features.

2.2 Windows 7 Installation

Unlike Windows Vista, Windows 7 installs with system reserved space (see Figure 1). System reserved space is 100mb and "hidden" partition (no drive letter) for the future implementation of BitLocker on the system. The volume is labeled "System Reserved" when viewed in device manager. The partition is created for booting, BitLocker and running the Windows Recovery Environment and the second partition is used for the operating system.

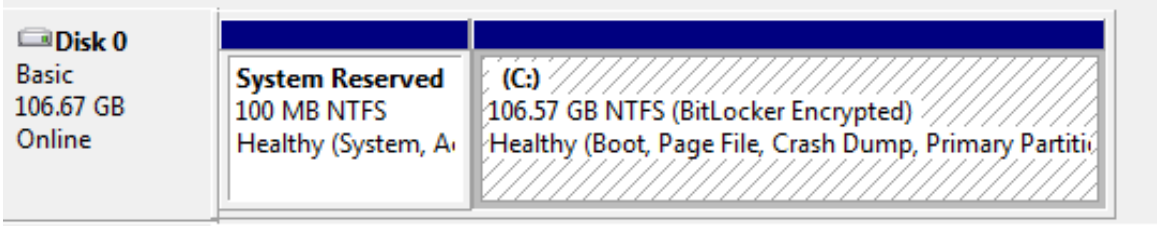


Figure 1: System Reserved Space

2.3 File System

The File System structure remains similar to Windows Vista and uses NTFS. When running on a solid-state drive (SSD), Windows® 7 requires a minimum of 16 gigabytes (GB) of space. Although some configurations of Windows 7 may appear to fit on smaller drives when initially installed, 8 GB SSDs are not sufficient for deploying Windows 7. Even when paired with a second drive of 4 or more GBs for application and data file storage, 8 GB hard drives do not allow for the increase in the Windows memory footprint that is expected to occur as users work on their computer. [1]

Some of the primary reasons for the increase over time in the Windows 7 memory footprint include:

1. Servicing - hard disk space must be reserved for software patches to the operating system and service-pack releases.
2. System Restore Points - restore points are automatically generated by Windows 7 and the amount of space required by default is relative to the size of the hard drive.

2.4 Libraries

Libraries are a Windows 7 feature that provides users a consolidated view of related files in one place. Users can search Libraries to find files quickly, even when those files are in different folders or on different systems (when those folders are indexed on the remote systems or cached locally by using Offline Files).

When a folder is removed from a Library, it only the removes the Library view of that folder. Removing a folder location from a Library doesn't actually delete the folder or its files.

Libraries can work with networks that are based on HomeGroups, workgroups, or domains, as long as users can access the shared folder on the network and that share is part of the Windows Search index on the remote system or that share is cached locally by

[1] http://technet.microsoft.com/en-us/library/dd744590(WS.10).aspx

using Offline Files. Windows 7 has a new feature called HomeGroup, which simplifies file sharing and networking.[2]

The Windows "Libraries" feature saves data to the following path:

C:\Users\<User_Name>\Appdata\Roaming\Microsoft\Windows\Libraries

Libraries are user-defined collections of content. A Library can display files that are stored in several folders at the same time. Libraries don't actually store items. They monitor folders that contain a user's items, and provide a single access point and rich view pivots (by file type, date or author) of this aggregated content. [3]

The Windows 7 default Libraries setting has one main Library called "Libraries" that contain four predefined default Libraries;

1. Documents,
2. Music,
3. Pictures, and
4. Videos.

Users can save and copy files directly to a library since every library has a default save location to send these files. Each library contains two physical file locations;

1. the user's personal folder, and
2. the public folder[4]

The properties of a Library are kept in an XML file with a '.library-ms' file extension. The properties files are found in the folder:

C:\Users\<User_Name>\ AppData\Roaming\Microsoft\Windows\Libraries

2.5 Restore Points

In Windows 7 there is no size limitation for restore points. Restore points are saved until the disk space System Restore reserves are filled up. Users can configure the amount of space used on the computer for System Restore by using the System Protection user interface on the System Properties dialog box (sysdm.cpl). System-image backups stored on an external hard disk can also be used for the purpose of restoring a system. Restore points have been broadened to the Application Level, and are recorded in the file properties of the file. To access the restore points, right click properties of the particular file.

[2] http://technet.microsoft.com/en-us/library/ee449413(WS.10)aspx
[3] http://windowsteamblog.com/windows/b/developers/archive/2009/04/06/understanding-windows-7-libraries.aspx
[4] ibid

In Windows 7, on computers with hard drives over 64 GB, System Restore can take up to 5 percent of the disk or a maximum of 10 GB of the disk space, whichever is less. On computers with hard drives of 64 GB or less, System Restore can take, at most, 3 percent of the disk space.[5]

Users can create additional system restore points and see exactly what files will be removed or added when a PC is restored.[6]

If users disable system protection (the feature that creates restore points) on a disk, all restore points are deleted from that disk. As with any type of deleted file, the restore point data should be able to be recovered. When users turn system protection back on, new restore points are created. Restore points are created automatically every week, and just before significant system events, such as the installation of a program or device driver. [7]

2.6 RAM Considerations

The Pagefile.sys and hiberfil.sys files increase in size in direct proportion to the amount of RAM installed on the computer. Windows 7 installations on 16 GB drives have a smaller memory footprint when the computer is limited to 1 GB of RAM. An increase of RAM to a size greater than 1 GB will result in increased size of the system files and less space on the hard drive for other applications and files. Increasing the size of the hard drive however, will not affect the size of these system files.[8]

2.7 Disk Defragmentation

One benefit of the Windows 7 defragmentation feature, in comparison to XP and Vista, is the ability to perform the defragmentation process on multiple drives simultaneously. This can be very useful for those who are used to performing defragmentation separately on their drives. Also, a new feature in Windows 7 defragmentation process is that it will automatically cancel any defragmentation started on a solid state disk. Also, note that flash memory doesn't need to be defragged.[9]

In Windows XP, the defrag rules were: *If a logical file was non-contiguous, then XP would defragment; this task could not be scheduled.* In Windows Vista, defragmentation only occurs for non-contiguous "chunks" larger than 64MB. Vista provided no User Interface (UI), and defragmentation could be scheduled a single volume at a time (serial

[5] http://msdn.microsoft.com/en-us/library/aa378910(VS.85).aspx
[6] http://www.microsoft.com/windows/windows-7/features/system-restore.aspx
[7] http://windows.microsoft.com/en-us/windows7/System-Restore-frequently-asked-questions
[8] http://technet.microsoft.com/en-us/library/dd744590(WS.10).aspx
[9] http://windows7.iyogi.net/features/enhancements/windows-7-defrag

processing). In Windows 7, a GUI was added back in, allowing for additional granularity of defragmentation settings, and multiple drives can now be defragmented in parallel.

2.8 Removable Media AutoPlay

Windows 7 has new configurable options for AutoPlay. Different media can be configured for unique handling. Windows 7 introduces key changes to AutoPlay that keep users from being inadvertently exposed to malware like Conficker when performing common tasks (e.g., locating files on a USB flash drive, downloading pictures from an SD card, etc.). [10]

In particular, Windows no longer displays the AutoRun task in the AutoPlay dialog for devices that are not removable optical media (CD/DVD) because there is no way to identify the origin of these entries. In Windows 7, U3 devices continue to emulate a CD for AutoRun access.

On the other hand, if a user inserts a CD that offers software to install, Windows will still display the AutoRun task provided by the Independent Software Vendor (ISV) during their media creation process.

2.9 Encrypted File System

Windows 7 offers an enhanced EFS scheme that is only supported in the *Professional*, *Enterprise* and *Ultimate* versions.

The Windows 7 EFS incorporates Elliptic Curve Cryptography (ECC) with backwards compatibility for RSA "mixed-mode" algorithms supported in previous Windows releases. ECC and RSA can be used together on the same system, and are configurable to allow only one type of encryption by domain policy.

Self signed certificates can be restricted and key lengths are defined by encryption technology: RSA: 1024bit – 16,384bit / ECC: 256bit – 531bit

2.10 Jump Lists

Jump Lists, like shortcuts, take users directly to documents, pictures, songs, or websites used routinely. To open a Jump List: ***right-click a program icon on the Windows 7 taskbar or find them on the Start menu***.[11]

Jump Lists are lists of recently opened items, such as files, folders, or websites, and are organized by the program that is used to open them.

[10] http://blogs.msdn.com/e7/archive/2009/04/27/improvements-to-autoplay.aspx
[11] http://windows.microsoft.com/en-us/windows7/products/features/jump-lists

Jump Lists are found in the User's profile at:

C:\Users\<User_Name>\AppData\ Roaming\Microsoft\Windows\Recent

There are two hidden subfolders in this directory:

1. AutomaticDestinations, and
2. CustomDestinations.

Files saved within these folders are saved with the extension 'automaticDestinations-ms' or 'customDestinations-ms'.

The Jump Lists keep track of the frequency and the "recentness" of the files accessed and displays them to the user in that order (using a weighted system, not just FIFO). Users can create their own custom Jump Lists. Jump List functionality can be turned off by the user; however, even when turned off the functionality continues to collect the information – it is just not displayed to the user. Jump Lists are also similar to the user assist keys.

2.11 Sticky Notes

Users may use Sticky Notes to write a to-do list, jot down a phone number, or do anything else that a pad of paper would be used for. Sticky Notes may be used with a tablet pen or a standard keyboard.[12] The Sticky Notes application is available only in the *Home Premium, Professional,* and *Ultimate* editions of Windows 7.[13]

Sticky notes are stored in a file titled as 'StickyNotes.snt'. The StickyNotes.snt file can be found in the following location:

C:\Users\<User_Name>\AppData\ Roaming\Microsoft\Sticky Notes

The content of the StickyNotes.snt files can include but is not limited to: sticky note content, when the note was created, nor when modified.[14]

2.12 The "Public" Account

There is a new account called "Public" that is accessible by any account and is stored in a separate folder.

The Public folders are a convenient way to share files on a user's computer. Users can share files in the Public folders with other users using the same computer and with users using other computers on the network. Any file or folder that a user places in a Public

[12] http://windows.microsoft.com/en-us/windows7/Using-Sticky-Notes
[13] http://windows.microsoft.com/en-us/windows7/products/features/sticky-notes
[14] http://www.simplecarver.com/exchange/articles/article-4.html

folder is automatically shared with users who have access to Public folders.[15] When Public folder sharing is turned on, users on the computer or network can access these folders. When turned off, only users with permissions have access.[16]

2.13 HomeGroup

A HomeGroup is a group of computers that share pictures, music, videos, documents, and printers. The computers must be running Windows 7 to participate in a HomeGroup.[17] HomeGroup allows a single login to administer the network from any connected Windows 7 computer. Full HomeGroup support is available with the *Home Premium, Professional, Enterprise* and *Ultimate* editions of Windows 7. The Starter and Home Basic editions can join HomeGroups, but not create them. HomeGroup offers more administrative control than workgroups.

2.14 Windows.old

Windows.old is a folder created during an upgrade to Windows 7. This folder contains the files, folders and drivers from previous windows versions. Windows.old folder may contain user data and settings from previous installed versions of Windows. [18]

Introduced in Windows Vista, Windows.old is created in an upgrade scenario as a backup mechanism during upgrade as a backup from a previous installation:

- Registry hives
- NTUSER.DAT
- Recycle bin

2.15 Internet Explorer V8

Windows 7 is distributed with Internet Explorer V8 as the default browser. The locations of the user data are similar to those in Internet Explorer 7.

2.15.1 "Index.dat" records

New Index.dat record types are created in IE8 and include:

- PrivacIE – InPrivacy Sessions (see Figure 2: PrivacIE)
- IECompat – IE compatibility mode – Appears to list IE compatible websites, published to the index.dat with out user interaction.
- Unknown - Not recognized by current utilities

[15] http://windows.microsoft.com/en-us/windows7/Share-files-using-the-Public-folders
[16] http://windows.microsoft.com/en-us/windows7/share-files-with-someone
[17] http://windows.microsoft.com/en-us/windows7/Share-files-using-the-Public-folders
[18] http://www.notebooks.com/2010/01/13/what-is-windows-old-folder-and-how-to-delete-it-safely/

Type		Last Visited [-0700]	User	URL
Unknown	☐	06/15/2009 12:38:31 Mon		PrivacIE:s-msn.com/i/5D/*/F0EBD554985A8CE6C61FD3E7359395.jpg
Unknown	☐	06/15/2009 12:38:32 Mon		PrivacIE:s-msn.com/i/41/*/7F454BF7B447B593C1969666C684CF.jpg
Unknown	☐	06/15/2009 12:38:31 Mon		PrivacIE:s-msn.com/i/25/*/29C9B2CA10702B9F35BADC2342119.jpg
Unknown	☐	06/15/2009 12:38:32 Mon		PrivacIE:s-msn.com/br/hp/*/wplay.png
Unknown	☐	06/15/2009 12:38:31 Mon		PrivacIE:s-msn.com/br/hp/*/WL_Hotmail_24x22_blue.gif
Unknown	☐	06/15/2009 12:38:32 Mon		PrivacIE:s-msn.com/br/hp/*/WindowsLive_Hotmail_logo_128x11_blue.gi
Unknown	☐	06/15/2009 12:38:31 Mon		PrivacIE:s-msn.com/br/hp/*/video.gif
Unknown	☐	06/15/2009 12:38:31 Mon		PrivacIE:s-msn.com/br/hp/*/tr_15.js
Unknown	☐	06/15/2009 12:38:31 Mon		PrivacIE:s-msn.com/br/hp/*/t.gif
Unknown	☐	06/15/2009 12:38:31 Mon		PrivacIE:s-msn.com/br/hp/*/ovr_37_kv_s.css
Unknown	☐	06/15/2009 12:38:31 Mon		PrivacIE:s-msn.com/br/hp/*/new.gif
Unknown	☐	06/15/2009 12:38:32 Mon		PrivacIE:s-msn.com/br/hp/*/msnbf.gif

Figure 2: PrivacIE

These user data records are found in 12 locations on Windows 7 installations, and located in the Users\<User_Name> path. In addition to the Users\<User_Name>, additional records can be found here:

1. C:\Users\<User_Name>\AppData\Local\Temp\Low\History\History.IE5\
2. C:\Users\<User_Name>\AppData\Local\Microsoft\Feeds Cache\
3. C:\Users\<User_Name>\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\
4. C:\Users\<User_Name>\AppData\Local\Microsoft\Windows\History\History.IE5\MSHist012009100520091006\
5. C:\Users\<User_Name>\AppData\Local\Microsoft\Windows\Temporary Internet Files\Low\Content.IE5\
6. C:\Users\<User_Name>\AppData\Local\Microsoft\Windows\History\History.IE5\
7. C:\Users\<User_Name>\AppData\Local\Microsoft\Windows\History\History.IE5\MSHist012009091420090921\
8. C:\Users\<User_Name>\AppData\Local\Microsoft\Windows\History\Low\History.IE5\
9. C:\Users\<User_Name>\AppData\Local\Microsoft\Windows\History\Low\History.IE5\MSHist012009100520091006\
10. C:\Users\<User_Name>\AppData\Roaming\Microsoft\Windows\Cookies\
11. C:\Users\<User_Name>\AppData\Roaming\Microsoft\Windows\PrivacIE\Low\
12. C:\Users\<User_Name>\AppData\Roaming\Microsoft\Windows\Cookies\Low\

Most settings will be located in the user's profile (Temp Internet Files, Favorites, Internet History)

C:\Users\<User_Name>\AppData\Local\Microsoft\Windows\History\History.IE5
C:\Users\<User_Name>\AppData\Local\Microsoft\Windows\History\Low\History.IE5

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

C:\Users\<User_Name>\AppData\Roaming\Microsoft\Windows\Cookies and Low folders
C:\Users\<User_Name>\AppData\Roaming\Microsoft\Windows\Cookies\Low

As in XP and Vista, examiners can still access Typed URLs at:

HKEY_USERS\<GUID>\Software\Microsoft\Internet Explorer\TypedURLS.

The setting to allow pop-ups is located in Registry Location

HKEY_USERS\<GUID>\Software\Microsoft\InternetExplorer\New window\Allow.

2.15.2 Clean up – (Clean My Tracks System Tools)

Internet Options – by default, IE8 will not automatically delete browser history when the browser is closed. When the IE8 clean up tools are run, they overwrite some index.dat files with zeros. The default settings in IE 8 are set to do the following:

Preserve Favorites Website Data – by default, this box is checked in IE8. When this is enabled, it will save the cookies and temporary Internet Files to those sites listed in the "favorites" folder.

Temporary Internet Files – files stored in the various TIF folders are deleted.

Cookies – cookies are deleted.

History – history of websites visited are deleted.

Form Data – saved information used in completing online forms are retained.

Passwords – saved passwords that are automatically filled in when visiting a previously visited website are retained.

InPrivate Filtering Data – InPrivate Filtering provides users an added level of control and choice about the information that third party websites can potentially use to track browsing activity. InPrivate Filtering data is retained.

The "Internet Options" page allows a user to reconfigure the settings for the browser. The user can delete the above listed areas manually or the "Internet Options" page can be set to delete the above listed options (the ones that are checked) as a batch. There is also the option, not on by default, to delete the browsing history upon exit of the browser (see Figure 3: Delete Browsing History).

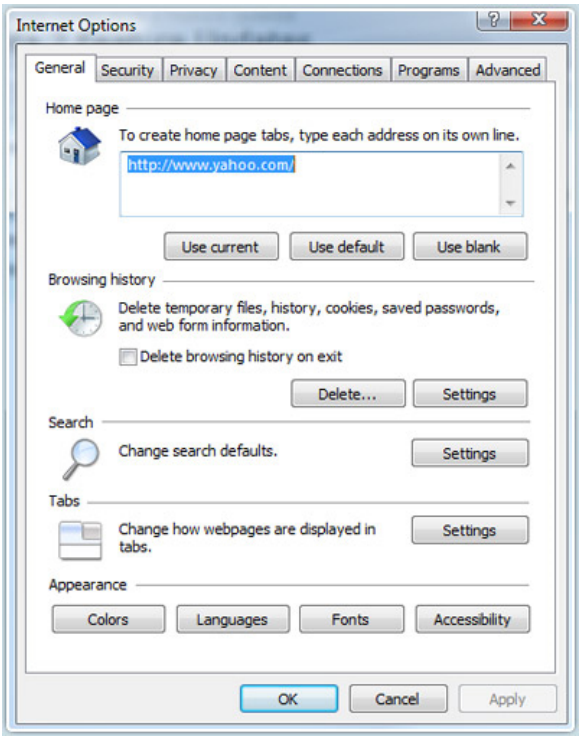


Figure 3: Delete Browsing History

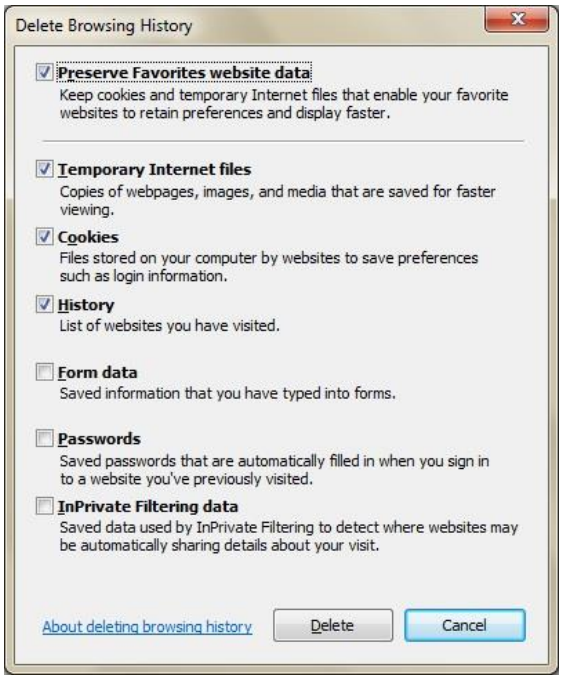


Figure 4: InPrivacy Browsing

IE8 allows a user to activate InPrivacy Browsing (Figure 4). This keeps a user's browsing history, temporary Internet files, form data, cookies, usernames and passwords from being retained by the browser and is designed to leave no evidence of browsing or search history after the browser is closed.[19]

[19] http://www.microsoft.com/windows-internet-explorer/readiness/new-features.aspx#history

2.16 BitLocker

BitLocker, available in the Ultimate and Enterprise editions, supports the encryption of entire volumes. Once BitLocker is enabled any file saved to that volume is encrypted automatically.

2.16.1 BitLocker To Go

BitLocker To Go—a new feature of Windows 7—gives the lockdown treatment to easily-misplaced portable storage devices like USB flash drives and external hard drives.[20]

2.16.2 BitLocker USB drives

The option to encrypt is available by simply right-clicking on a drive in Windows Explorer to enable BitLocker protection. With BitLocker To Go, you can encrypt removable storage devices, such USB flash drives. All you need to do is right-click on the drive you want to protect, select the "Turn on BitLocker" menu option, and follow the basic wizard.

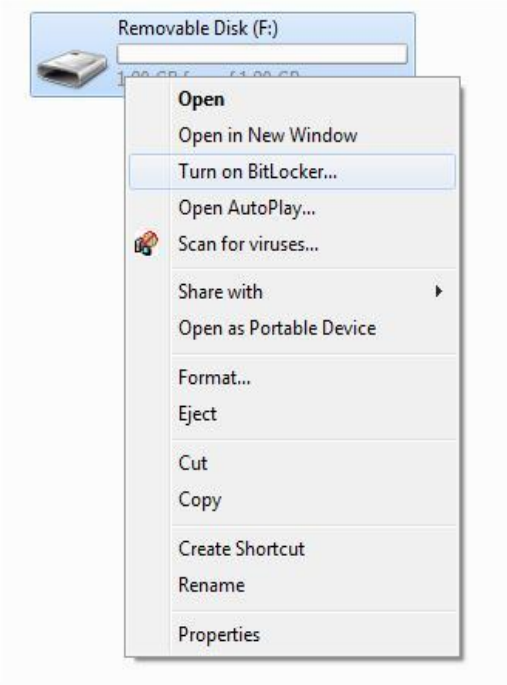


Figure 5: BitLocker USB Drives

[20] http://windows.microsoft.com/en-us/windows7/products/features/bitlocker

2.16.3 Auto Unlock

When selecting "unlock the drive automatically" an auto-unlock registry key is created at the following registry location.

HKCU\Software\Microsoft\Windows\CurrentVersion\FVEAutoUnlock\<GUID>

RegSetValue – REGBIN – element
RegSetValue – REGBIN – info

A BitLocker To Go device is set to auto-unlock if there are GUIDs present.[21]

2.16.4 BitLocker To Go support for Windows XP and Vista

Using BitLocker To Go Reader, BitLocker encrypted devices can be used on Windows XP and Vista computers. BitLocker To Go Reader doesn't allow you to encrypt drives using BitLocker or add files to an encrypted drive. It only allows a user to read files on a BitLocker encrypted drive plugged in to a computer running Windows Vista or Windows XP.

2.17 Virtualization

Windows Virtualization Support original was only offered on computers which supported hardware virtualization. Windows Virtualization Support is now available on all computers running Windows 7.

2.17.1 Windows XP Mode

Windows 7 Professional and above allow the use of Windows XP Mode. Windows XP Mode is designed to utilize Business Legacy Applications that are not supported by Windows 7. The Distribution of Windows 7 comes with a license to use Windows XP, for virtualization.

Once installed Windows XP Mode short cuts can be dragged to the Windows 7 Desktop. Then the XP application can be launched directly from Windows 7. The short cut path will reference the XP Mode virtual hard disk location where the application resides.

The System event logs record the launch of the virtual session (see Table 1: System Event Log). Event 222 records the user name, application launched, the date and time the session was run. Event logs are stored as .xml data.

[21] http://technet.microsoft.com/en-us/library/ee424320%28WS.10%29.aspx

Table 1: System Event Log

Item	Event
Log Name	Microsoft-Windows-Virtual PC/Admin
Source	Microsoft-Windows-Virtual PC
Date	9/4/2009 3:33:44 PM
Event ID	222
Task Category	None
Level	Information
Keywords	
User	Computer_Name_PC\User
Computer	Computer_Name_PC
Description	A virtual application {Microsoft.NET Framework 1.1 Wizard} was published from the VM running {Windows® XP Professional} with IC version {14.0.7234.0} on a {en-US} trust

2.17.2 VHD Support in Windows 7

In addition to allowing for the mounting of Virtual Hard Disk (.VHD) files using Virtual PC, Windows 7 has native support for .VHD. Windows 7 Explorer can mount .VHD files. A user can boot directly to .VHD images on a Windows 7 volume. Booting to .VHD has some limitations, it does not support hibernation and BitLocker cannot be used on host or guest operating systems. The .VHD must not be housed on a compressed volume or in a compressed folder

By default Virtual Hard Drive files are found in the following paths, however these can be configured to other locations by the user:

C:\Users\<User_Name>\AppData\Local\Microsoft\Windows Virtual PC\Virtual Machines\Windows XP Mode.vhd

C:\Users\<User_Name>\Virtual Machines\

The .VHD is seen as a single file by forensic utilities and can be searched and data carving can be used. A .VHD can also be mounted in a write protected session for additional examination.

Windows 7 provides a Virtual Machine Management tool GUI. The tool allows for permissions to be set for sharing and read/write management. VHDs can be shared with, Nobody, Homegroup/Network (read), Homegroup/Network (read/write), and Specific Users (see Figure 6: Windows XP Mode).

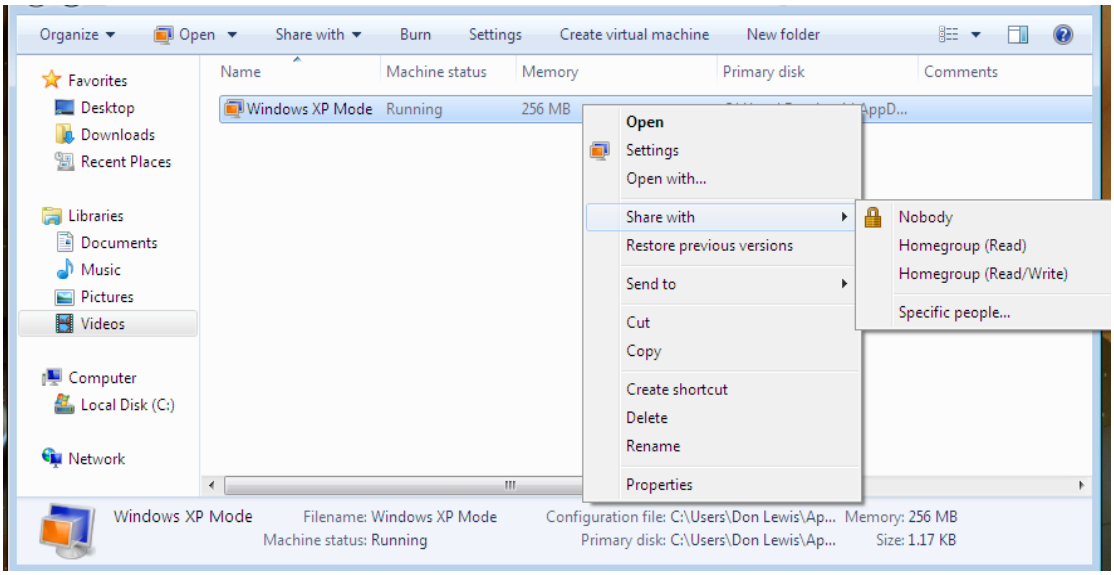


Figure 6: Windows XP Mode

2.18 Solid State Media

Disk Defragmentation, Superfetch, boot prefetching, application launch prefetching, ReadyBoost and ReadDrive are all disabled for Solid State Media in Windows 7. Windows 7 has turned off Windows Disk Defragmenter in order to take advantage of the capabilities and unique performance characteristics of solid-state drives.[22]

Solid State Drives can be identified in Windows 7 using one of the following methods:

1. A command is sent to the drive using ATA as defined by ATA8-ACS Identify Word 217. When queried, the device reports back its Nominal Media Rotational Rate as: "Non-Rotational media" or 0001h.
2. If a system disk reports a random read performance characteristic above the threshold of 8 MB/sec.

Once a drive is successfully identified as being Solid State media, the following are disabled:

- Disk Defragmentation
- Superfetch
- Boot prefetching
- Application launch prefetching
- ReadyBoost
- ReadDrive

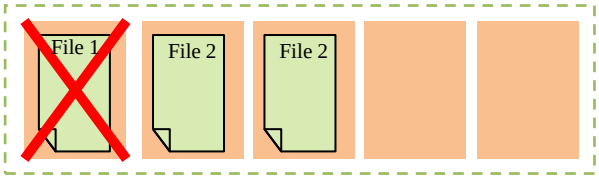
[22] http://windows7.iyogi.net/features/enhancments/file-system-in-windows-7

2.19 TRIM Command

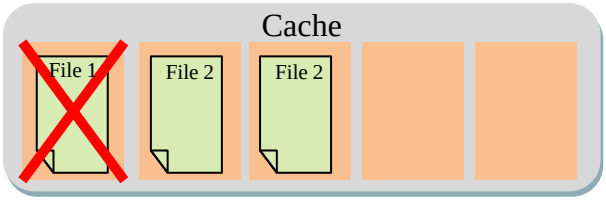
TRIM (with proper OS and drive support) will effectively let the OS tell the SSD to wipe invalid pages before they are overwritten. Implementation of this command is important to note for forensic examiners as it may permanently delete data. An example of TRIM follows:

Example: A 4k file (File 1) is written to SSD media. Immediately after that, an 8k file (File 2) is written to that same block. If File 1 is then deleted, and TRIM is supported, the following steps occur:

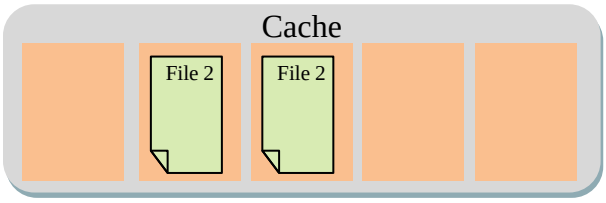
1. File 1 is marked as deleted by the operating system.



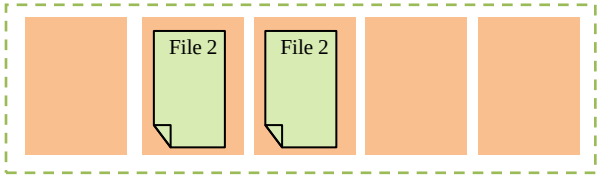
2. The entire block is read and written to Cache.



3. File 1 is replaced by 00h in Cache



4. The entire block is written from Cache to the media.



It should be noted the blocks being written from Cache to the media may not be written to their original block. Therefore with the appropriate tools data files may be recovered from their original blocks.

- TRIM cannot be invoked when overwriting a file (e.g. adding data to an existing document).

- TRIM is NOT a Microsoft specific operation and is currently supported in the Linux 2.6.28 kernel and Windows Server 2008 R2.ou

History
SWGDE Technical Notes on Microsoft Windows 7

Revision	Issue Date	Section	History
1	June 2010		Original Release for Public Comment
1	--		Updated document per current SWGDE Policy with new disclaimer. No changes to content and no version/publication date change. (9/27/2014)