Scientific Working Group on Digital Evidence

SWGDE Windows 8 and 8.1 Tech Notes

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.

SWGDE Windows 8 and 8.1 Tech Notes

Table of Contents

1. Scope

The scope of this document is to identify differences between previous Microsoft operating systems and Microsoft Windows® 8/8.1 as it applies to digital forensics, software, and hardware tools. This document is an overview of the new Windows 8/8.1 software.

2. Overview of Windows 8

Microsoft made Windows 8 available for retail sales on October 26, 2012. Public sales of Windows 8 ended on October 31, 2014 and sales of computers with Windows 8 ended on June 30, 2016. Public support of Windows 8 ended on October 31, 2014. Windows 8 support is extended through its update to Windows 8.1. Support for new chipsets has limited support.

(http://windows.microsoft.com/en-us/windows/lifecycle)

Windows 8 introduces major changes to the operating system's graphical user interface (GUI) to improve its user experience. These changes include a touch-optimized Windows shell based on Microsoft's "Metro" design language, the Start screen displays programs and dynamically updated content on a grid of tiles.

Windows 8 allows the user to sign into their operating system using either a Microsoft Account or a Local Account. The Microsoft Account consists of an e-mail address and a password; this allows a user to download Apps from the Windows Store and run all the bundled Apps in Windows 8. A user can also link a Microsoft account with their social media accounts, automatically stocking address book with friends from Facebook, Twitter, and other sites.

2.1 Versions

Windows 8 has four editions:

1. Windows 8 (Core);
2. Windows 8 Pro;
3. Windows RT;
4. Windows 8 Enterprise.

Windows 8.1 has the same four editions:

1. Windows 8.1 (Core);
2. Windows 8.1 Pro;
3. Windows RT 2;
4. Windows 8.1 Enterprise.

Windows 8/8.1 also provides a local language-only edition for China and a small set of select emerging markets.

With the exception of Windows 8 RT/RT2, all of these operating systems are offered in both 32-bit and 64-bit. The Windows 8/8.1 (Core) 32-bit systems supports a maximum of 4GB of RAM,

and the 64-bit Windows 8/8.1 (Core) systems supports a maximum of 192GB. Windows 8/8.1 Pro and Enterprise 64-bit systems supports 512GB of RAM. Windows RT/RT2 supports a maximum of 4GB of RAM.

2.1.1 Windows 8/8.1 (Core)

Windows 8 is the basic edition of Windows 8 and contains basic features aimed at the home market segment. It provides all of the basic new Windows 8 features.

2.1.2 Windows 8/8.1 Pro

Windows 8/8.1 Pro contains features geared towards power and business users. These additional features include Remote Desktop connections, ability to connect to a Windows domain, Encrypting File System (EFS), Hyper-V, Virtual Hard Disk Booting, Group Policy, BitLocker, and BitLocker To Go. The Windows Media Center is an add-on to the Pro version.

2.1.3 Windows 8/8.1 Enterprise

Windows 8/8.1 Enterprise is available to Microsoft's Software Assurance customers, and MSDN and Technet Professional subscribers. It provides all the features in Windows 8/8.1 Pro, except the ability to install the Windows Media Center add-on, with additional features to assist with IT administration.

2.1.4 Windows RT/RT2

Windows RT/RT2 is only available on 32-bit ARM devices, such as tablet PCs. It includes touch-optimized desktop versions of the basic set of the Microsoft Office 2013 applications. It supports device encryption. Software applications for Windows RT are available on the Windows Store and are based on the Windows Runtime API, which differs from traditional Microsoft Apps.

2.2 Windows 8 Installation

Like Windows 7, Windows 8 installs with a System Reserved partition; the size of this partition has been increased to 350MB for the future implementation of BitLocker on the system. The volume is labeled "System Reserved" when viewed in Device Manager and is not assigned a drive letter. The partition is used for booting, BitLocker, and running the Windows Recovery Environment. A second partition is used for the operating system. Installation typically creates an additional 8-15GB hidden partition with a Microsoft recovery image of a fresh install. The Microsoft recovery image is read when a user selects a recovery option in settings.

The default partition structure is listed below, though users may customize this during installation:

- Windows (core OS - NTFS)
- Recovery (NTFS)

- Reserved, System (UEFI - FAT 32)
- Recovery Image (NTFS)

2.3 File System

The file system structure remains similar to Windows 7 and uses NTFS. Installation of Windows 8 requires a minimum of 16GB of space for a 32-bit installation, and 20GB for a 64-bit installation.[1] Windows 8 supports NTFS, FAT32, and exFAT file systems. Windows 8.1 brought the Resilient File System (ReFS) to the consumer market, which is a Microsoft proprietary file system introduced in Windows Server 2012 with the intent of being the next generation of NTFS. ReFS adds improved reliability for on-disk structures, built-in resilience, and compatibility with existing APIs and technologies.

2.4 Libraries

As in Windows 7, Libraries provide 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 computers (when those folders are indexed on the remote systems or cached locally by using Offline Files).

When a folder is removed from a Library, this only the removes the Library view of that folder. Removing a folder location from a Library does not delete the folder or its files. Libraries can contain shared folders from remote systems, provided users can access the shared folder on the network, and that share is part of the Windows Search index on the remote system or cached locally using Offline Files.

Certain Metro Apps, such as the default Photos App, can only access files in Libraries.[2]

The Windows "Libraries" feature saves data to the following path:
C:\Users\<User_Name>\Appdata\Roaming\Microsoft\Windows\Libraries

Windows 8 has four predefined Libraries: Documents, Music, Pictures, and Videos.

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 and File History

In Windows 8, there is no size limitation for restore points. Restore points are saved until the disk space System Restore reserves are filled. Users can configure the amount of space used on the computer for System Restore using the System Protection user interface on the System

[1] http://atechjourney.com/minimum-requirement-for-installing-windows-8.html/
[2] http://www.makeuseof.com/tag/understand-windows-8-libraries-master-storage-space/

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.

Windows 8 provides an optional backup facility, File History, that replaces the Windows Backup and Restore functions in Windows 7; File History is not enabled by default. If enabled, File History backs up contents of a user's libraries, favorites, contacts, and desktop to a user-specified location, such as an external drive or network location. File History backups exclude OneDrive (SkyDrive) files (unless they are made available offline), EFS-encrypted files and folders, and files and folders not contained in libraries. File History relies on the Windows Search service. Unlike most backup applications, File History does not require Administrative rights to configure, and to backup or restore files.

By default, System Restore uses the lesser of 5% of disk space or 10 GB on disks larger than 64 GB, and 1-3% of disk space on smaller disks.

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 may be able to be recovered. When users enable System Protection, 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. Using the System Protection user interface, users can create additional restore points and see what files will be removed or added when a PC is restored to a restore point.

2.6 Storage Spaces

Storage Spaces in Windows 8 allows combining multiple hard disk drives (HDDs) or solid state drives (SSDs) of different sizes and interfaces into one storage pool. A Storage Space is actually a virtual disk and it is usable in Windows just like any other drive.

2.7 RAM Considerations

Windows 8 has the same memory requirements as Windows 7; however, it uses memory more efficiently. Microsoft designed Windows 8 to require just 200MB of memory, minus any display memory requirements. Microsoft achieved the reduction in the footprint by

1. Removing duplicates of values in memory and maintaining a single copy;
2. Removing 13 startup services, changing others to “manual start” and “startup on demand”;
3. Removing low-level OS components dating back to the NT-era by the re-architecture of code to separate frequently referenced data structures from infrequently referenced data structures;
4. Removing the Windows desktop from Windows shell which saves about 23MB of RAM; and

5. Changing the prioritization of memory usage.[3]

When Hibernation and Fast Boot are enabled (which is the default setting), the hiberfil.sys file will take approximately three-fourths of RAM. In previous versions of Windows, the hiberfil.sys file stored the kernel session, device drivers, and application data. In Windows 8, the hiberfil.sys file stores the kernel session and device drivers only, and the file remains more or less constant.

In Windows 8 the swapfile (swapfile.sys) is not used during the Fast Startup process. Instead, the swapfile is used internally by the system to make certain types of paging operations more efficient, and it is used to suspend or resume Metro or Modern Windows 8 Apps.

2.8 Disk Defragmentation

By default, Windows 8 only defragments files smaller than 64MB, which means that large media and game files are left untouched. In order to defragment files of all sizes, the *-w* parameter should be used with the command line utility. While Windows 7 turned off defragmentation for solid state drive (SSD), Windows 8 has enables defragmentation by default for SSDs.

2.9 Prefetch and SuperFetch

Windows uses Prefetch Files (PF) to improve application startup performance by loading application data into memory before it is demanded. Windows creates a Prefetch file when an application is run from a particular location.

Prefetch files are all named in a common format where the name of the application is listed, then an eight character hash of the location where the application was run, followed by the .PF extension. For example, the Prefetch file for calc.exe would appear as CALC.EXE-0FE8F3A9.pf, where 0FE8F3A9 is a hash of the path from where the file was executed. These files are all stored in the root of the Windows\Prefetch\ folder.

Windows 8 uses SuperFetch which is a technology that allows Windows to manage the amount of RAM in the machine it runs on more efficiently by making sure often-accessed data can be read from the fast RAM instead of the slow hard drive.

SuperFetch is implemented in Sysmain.dll as a Windows service that runs inside a Service Host process (Svchost.exe). The files can be found in: C:\Windows\Prefetch\.

The scheme relies on support from the Memory Manager so that it can retrieve page usage histories as well as direct the Memory Manager to preload data and code from files on disk or from a paging file into the Standby List and assign priorities to pages.

The SuperFetch service extends page-tracking by tracing, using traditional page aging mechanisms in Memory Manager, the page data and code that was once in memory. It stores this information in scenario files with a .DB extension in the %SystemRoot%\Prefetch directory

3 http://winsupersite.com/windows-8/windows-8-and-reduced-memory-usage

alongside standard Prefetch files used to optimize application launch. Using this deep knowledge of memory usage, SuperFetch can preload data and code when physical memory becomes available.[4]

Whenever memory becomes free, for example when an application exits or releases memory, SuperFetch asks the Memory Manager to fetch data and code that was recently evicted. This is done at a rate of a few pages per second with Very Low priority I/Os so that the preloading does not impact the user or other active applications.

SuperFetch also includes specific scenario support for hibernation, standby, Fast User Switching (FUS), and application launch. When the system hibernates, for example, SuperFetch stores data and code in the hibernation file that it expects (based on previous hibernations) will be accessed during the subsequent resume.[5]

2.10 Removable Media AutoPlay

Windows 8 continues the AutoPlay feature, which was first introduced in Windows 7. AutoPlay allows a user to choose an action for different kinds of media after removable media is inserted or attached to the Windows 8 host system. A user can set AutoPlay to open different kinds of content, such as pictures, music, and video on a variety of media.

2.11 Encrypted File System

Windows 8 offers an enhanced EFS scheme that is only supported in the *Professional* and *Enterprise* versions. The Windows 8 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: 1024-bit – 16,384-bit / ECC: 256-bit – 521-bit. By default, RSA key lengths are 2048-bit for self-signed certificates and 256-bit for ECC certificates.

EFS works on the file level in the NTFS filesystem rather than encrypting the entire disk. BitLocker[6] is the preferred method to encrypt full disks in Windows 8. Several weaknesses have been found with EFS allowing decryption of data. Copying files to an external drive automatically removes the EFS encryption. Windows 8 improves robocopy adding a switch /EFSRAW to copy EFS files and maintains their encryption. EFS requires a recovery agent

[4] Windows Internals Part 2, Microsoft Press
[5] https://technet.microsoft.com/en-us/magazine/cc162480.aspx
[6] BitLocker Drive Encryption is a data protection feature available in Windows 8 Pro, Windows 8 Enterprise, and in all editions of Windows Server 2012. BitLocker encrypts the hard drives on your computer to provide enhanced protection against data theft or exposure on computers and removable drives that are lost or stolen, and more secure data deletion when BitLocker-protected computers are decommissioned as it is much more difficult to recover deleted data from an encrypted drive than from a non-encrypted drive.

different from the file owner which allows an administrator to circumvent the encryption. Some built in features such as indexing and file history ignore EFS encrypted files.

2.12 Jump Lists

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.

Windows 7 previously used Start Menu and taskbar jump lists. However, in Windows 8, since the Start Menu no longer exists, only the taskbar jump lists remain. Jump lists are used by pinned items on the taskbar to capture recently opened items. Windows Explorer searches can also be saved in jump list format and pinned to the taskbar.[7]

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 display 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, though it is not displayed to the user. Jump Lists are also similar to the user assist keys.

2.13 Sticky Notes

Microsoft removed the Sticky Notes application from the default installation of Windows 8, and users now can download it free from the Microsoft store.

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 and/or modified.

2.14 The "Public" Account

Microsoft continues the "Public" account in Windows 8, which 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

[7] http://www.technorms.com/27427/work-jump-lists-windows-8

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 folder is automatically shared with users who have access to Public folders. 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.

2.15 HomeGroup

A HomeGroup is a group of computers that can share pictures, music, videos, documents, and printers. In order to join a HomeGroup, the computer must be running at least Windows 7. Systems running Windows RT 8.1 can join a HomeGroup; however, users from a system running Windows RT 8.1 cannot create a HomeGroup.[8]

2.16 Windows.old

Windows.old is a folder created during an upgrade to Windows 8. 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.[9] According to Microsoft, if you choose to "Keep nothing" when you upgrade to Windows 8.1, or if you reset, refresh, or reinstall Windows, your personal files are temporarily saved to the Windows.old folder for 28 days (unless you formatted your hard drive before installing). If you decide you want some or all of these files back, you can usually retrieve them from this folder.[10]

2.17 Internet Explorer V10

Windows 8 is distributed with Internet Explorer V10 (IE10) as the default browser, which uses a completely revised file structure to store browsing data.

2.17.1 Cache/History Information

Microsoft replaced the index.dat file in IE10 to a single ESE (Extensible Storage Engine) database or .edb file. The database file (WebCacheV24.dat) is located under C:\Users\<User_Name>\AppData\Local\Microsoft\Windows\WebCache folder[11]

This folder contains the following files which work together to index the Internet Explorer history:

[8] http://windows.microsoft.com/en-us/windows/homegroup-help#homegroup-start-to-finish=windows-81&v1h=win81tab1&v2h=win7tab1

[9] http://www.notebooks.com/2010/01/13/what-is-windows-old-folder-and-how-to-delete-it-safely/

[10] https://support.microsoft.com/en-us/help/17125/windows-8-restore-files-old-folder-upgrade

[11] http://blog.nirsoft.net/2012/12/08/a-few-words-about-the-cache-history-on-internet-explorer-10/

Table 1. Internet Explorer History Files

File type:	Filename:
Checkpoint file	V01.chk
Transaction log file	V01.log
Reserved transaction log file	V01res#####.jrs
Reserved transaction log file	V01res#####.jrs
Transaction log file	V01#####.log
ESE database	WebCacheV01.dat

[12]

Browsing data is not directly stored in the ESE data; however, it is first stored in a log buffer within a storage container in RAM. The default size for the log buffers is the same as the disk sector size and the minimum amount of log buffers are 128 sectors and the maximum amount being 10,240 sectors, which is approximately 5.2MB. As the log buffers reach maximum capacity, the data is then written from RAM to disk within the log files.[13]

Power loss may result in losing data from these RAM log buffers that have not been committed to disk.

The ESE database is made up of containers which group the following types of browsing data: cookies, downloads, visited URLs, cache and history. User data records are found in 16 locations on Windows 8 installations, and located in the Users\<User_Name> path. The paths for these locations are found in TABLE 2.

Table 2. User Data Record Locations

[12] https://articles.forensicfocus.com/2013/12/10/forensic-analysis-of-the-ese-database-in-internet-explorer-10/
[13] https://articles.forensicfocus.com/2013/12/10/forensic-analysis-of-the-ese-database-in-internet-explorer-10/

1. C:\Users\<User_Name>\AppData\Local\Microsoft\Internet Explorer\IECompatData\
2. C:\Users\<User_Name>\AppData\Local\Microsoft\Internet Explorer\IEFlipAheadCache\
3. C:\Users\<User_Name>\AppData\Local\Microsoft\Windows\WebCache\
4. C:\Users\<User_Name>\AppData\Local\Microsoft\Windows\History\
5. C:\Users\<User_Name>\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\
6. C:\Users\<User_Name>\\AppData\Local\Microsoft\Windows\Temporary Internet Files\Low\Content.IE5\
7. C:\Users\<User_Name>\AppData\LocalLow\Microsoft\Internet Explorer\DOMStore\
8. C:\Users\<User_Name>\AppData\Roaming\Microsoft\Windows\Cookies\
9. C:\Users\<User_Name>\AppData\Roaming\Microsoft\Windows\Cookies\Low\
10. C:\Users\<User_Name>\AppData\Roaming\Microsoft\Windows\IECompatCache\
11. C:\Users\<User_Name>\AppData\Roaming\Microsoft\Windows\IECompatCache\Low\
12. C:\Users\<User_Name>\AppData\Roaming\Microsoft\Windows\IECompatUACache\
13. C:\Users\<User_Name>\AppData\Roaming\Microsoft\Windows\IECompatUACache\Low\
14. C:\Users\<User_Name>\AppData\Roaming\Microsoft\Windows\IEDownloadHistory\
15. C:\Users\<User_Name>\AppData\Roaming\Microsoft\Windows\PrivacIE\
16. C:\Users\<User_Name>\AppData\Roaming\Microsoft\Windows\PrivacIE\Low\

As in XP, Vista and Windows 7 versions, examiners can still access Typed URLs at: HKEY_USERS\<GUID>\Software\Microsoft\Internet Explorer\TypedURLS. Windows 8 adds another key call "TypedURLSTime" which contains hex values indicating the date/time the TypedURL was entered.[14]

The setting to allow pop-ups is located in Registry Location: HKEY_LOCAL_MACHINE\Software\Microsoft\Internet Explorer\Main\FeatureControl \FEATURE_WEBOC_POPUPMANAGEMENT.

2.17.2 Location of IE10 Data

- Bookmarks are stored in separate Internet Shortcut (.url) files within the 'Favorites' folder.
- Cache records are stored in the 'WebCacheV01.dat' ESE database, within the 'Content' containers. The cached files are stored as separate files in locations specified within the ESE database.
- Cookies are stored in the 'WebCacheV01.dat' ESE database, within the 'Cookies' containers. The cookie files are stored as separate files in locations specified within the ESE database.
- Downloads are stored in the 'WebCacheV01.dat' ESE database, within the 'IE download' containers.

[14] http://computerforensicsblog.champlain.edu/2012/04/11/windows-8-forensics-part-2/

- Session Data is stored in a number of .dat files within the 'Recovery' folder.
- Website Visits are stored in the 'WebCacheV01.dat' ESE database, within the 'History' containers.

2.17.3 Delete Browser History

By default, IE10 will not automatically delete browser history when the browser is closed. When the IE10 cleanup tools are run, they overwrite some index.dat files with zeros. The "Internet Options" page allows a user to reconfigure the settings for the browser. The user can delete the below listed areas manually or the "Internet Options" page can be set to delete the below 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.

The default settings in IE10 are set to do the following:

- **Preserve Favorites Website Data** – by default, this box is checked in IE10. When this is enabled, it saves the cookies and temporary Internet Files to those sites listed in the "favorites" folder.
- **Temporary Internet Files (TIF)** – 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 are automatically filled in when re-visiting a previously visited website.
- **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.

IE10 allows a user to activate InPrivate Browsing mode. 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.

2.18 BitLocker

BitLocker, available in the Windows 8 Pro and Windows 8 Enterprise editions, supports the encryption of entire volumes. Once BitLocker is enabled any file saved to that volume is encrypted automatically.

Windows 8 introduces the ability to encrypt used disk space only as opposed to the entire volume. Also introduced is the ability to enable BitLocker during installation of Windows 8, support for encrypted hard drives, and brute force protection. Brute force protection is an optional feature which places the device in BitLocker recovery mode when a brute force attack on the Windows sign-in is detected.

BitLocker To Go and Auto Unlock, introduced with Windows 7, remain as features of Windows 8. BitLocker To Go gives the lockdown treatment to easily-misplaced portable storage devices like USB flash drives and external hard drives. Auto Unlock, another optional feature, creates a registry key at the following location when enabled: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\FveAutoUnlock.[15]

2.19 Virtualization

Both 32 and 64 bit versions of Windows 8 include Hyper-V as a virtualization platform. However, only the 64-bit version can create a virtual machine (VM). Hyper-V is not enabled by default.

Windows 8 introduces support for a new version of virtual disk, VHDX, though it still supports the prior version, VHD. VHD supported a maximum of 2TB; VHDX supports virtual disks up to 64TB. VHDX format incorporates built-in protections against file corruption by tracking file updates in the metadata. The VHDX format improves performance over the legacy format when disks are expanded.

Another feature is Hyper-V's "Live Storage Move" capability, which allows a user to move the VM's storage from one local drive to another, to USB storage media, or to a remote file share without needing to stop the VM.

Hyper-V also has the ability to take "snapshots" of a running VM. A "snapshot" saves everything about the VM machine state and allows the user to revert back to a previous state.[16]

2.20 Solid State Drives

If the Windows System Assessment Tool (WinSAT) detects a Solid State Drive (SSD), it sets the appropriate optimization settings for SSDs. When Windows 8 is installed "fresh" on a SSD, WinSAT runs automatically. When Windows 8 volume is moved from a traditional disk to a SSD, optimal settings may not be set. Under Windows 7, execution of WinSAT could be detected by observing the Windows Experience Index (WEI) score. In Windows 8.1, this score is not displayed. To optimize the system for an SSD, WinSAT needs to be run and the system rebooted.

2.20.1 Trim Command

SSDs are storage devices comprised of flash memory. SSDs can be written to on a byte level, but must be erased at a block level. Introduced in Windows 7, trim is a storage level hint to inform Windows is not using certain regions. NTFS sends trim hints when files are deleted or moved. SSDs consume these trim hints through a background process called 'reclaim' that prepares the drives for next writes. SSDs may perform these optimization tasks immediately, store the hints for later processing, or discard the hints for lack of time to perform the task immediately. At idle

[15] https://technet.microsoft.com/en-us/library/dn306081.aspx
[16] https://blogs.msdn.microsoft.com/b8/2011/09/07/bringing-hyper-v-to-windows-8/

time, the Storage Optimizer, the new defragmentation tool in Windows 8, sends a complete set of trim hints for the entire volume on the SSD again. This creates a better chance for the SSD to react to the hints and increases its performance and optimization.

2.20.2 SuperFetch, ReadyBoot, ReadyBoost Services on SSDs

SuperFetch is a performance enhancement implemented in Windows Vista and later versions of Windows to reduce the time necessary to launch applications. See section 2.8 for a more detailed explanation of Superfetch. ReadyBoost and ReadyBoot work together to speed up the process of booting the system and recovering from hibernation. If the system drive is a fast SSD, as measured by the Windows Experience Disk score, then SuperFetch turns off ReadyBoot, ReadyBoost, and the SuperFetch service itself.

2.21 Windows To Go

Windows To Go is an enterprise feature in Windows 8 that enables users to create a portable workspace that can be booted from USB device on another machine regardless of that machine's OS. Windows To Go operates just like any other Windows 8 installation with a few exceptions[17]:

- **Internal disks are offline.** To ensure data isn't accidentally disclosed, internal hard disks on the host computer are offline by default when booted into a Windows To Go workspace. Similarly if a Windows To Go drive is inserted into a running system, the Windows To Go drive will not be listed in Windows Explorer.
- **Trusted Platform Module (TPM) isn't used.** When using BitLocker Drive Encryption a pre-operating system boot password will be used for security rather than the TPM since the TPM is tied to a specific computer and Windows To Go drives will move between computers.
- **Hibernate is disabled by default.** To ensure that the Windows To Go workspace is able to move between computers easily, hibernation is disabled by default. Hibernation can be re-enabled by using Group Policy settings.
- **Windows Recovery Environment isn't available.** In the rare case that you need to recover your Windows To Go drive, you should re-image it with a fresh image of Windows.
- **Refreshing or resetting a Windows To Go workspace is not supported.** Resetting to the manufacturer's standard for the computer doesn't apply when running a Windows To Go workspace, so the feature was disabled.
- **Getting Apps from Windows Store.** For Windows To Go images that are running Windows 8.1, there is no difference in Windows Store behavior between a standard

[17] https://technet.microsoft.com/en-us/library/hh831833(v=ws.11).aspx#wtg_hardware

Windows installation and a Windows To Go installation. Store Apps can roam between multiple PC's on a Windows To Go drive.

Windows To Go is a full operating system that can be populated with a full range of applications, just as a traditional installation.

Microsoft recommends Windows To Go certified USB drives which have been optimized to run a full OS from a USB drive. Windows To Go certified USB drives ensure devices are built for high random read/write speeds and support the thousands of random access I/O operations per second required for running normal Windows workloads smoothly. Windows To Go certified USB drives have been tuned to ensure they boot and run on hardware certified for use with either Windows 7 or Windows 8. Windows To Go certified USB drives are built for long term use and are supported with manufacturer warranties.

Even though not officially supported by Microsoft, users can install non Windows To Go Certified devices.[18]

2.22 Modern Apps

Windows 8 introduces the Metro UI and with it a new classification of applications referred as *Modern Apps*. Later as Windows application development changed, these would be referred to as *Windows Runtime Apps* and eventually *Windows Universal Apps*. Windows 8 provides support for traditional apps or apps developed to run on .NET, however the classic application runs in the desktop environment and are distributed outside the Windows Store. *Windows Runtime Apps* have security restrictions similar to Android and iOS apps where users can restrict or grant access to build in security domains. For example, an application typically is restricted to writing only to the application's AppData folder but could require through its manifest access to user's Picture library for an embedded functionality.

Greater restrictions were put in place for applications communicating with other applications, a process known as interprocess communications, or IPC. *Modern Apps* are sandboxed and unable to communicate outside their security domain. After realizing how completely sandboxing Apps restricted Windows 8 in the enterprise environment, Microsoft added IPC support through brokered services for Windows sideloaded Apps. Windows 8.1 update includes support for *Brokered Services*. Windows apps implementing brokered services require .NET 4.5+ or newer bindings. Microsoft apps with brokered services fail Windows Store certification, however this provides a means for enterprises to migrate their internal applications to Windows 8.1 while taking advantage of the Modern UI.

[18]http://forums.appleinsider.com/discussion/186425/how-to-boot-windows-on-a-thunderbolt-external-drive

2.23 Powershell

Powershell is an automation and interactive management framework complete with an object oriented scripting language and command line shell. With each release of Windows since XP, Microsoft has released a new version of Powershell. Powershell 3.0 released with Windows 8. Windows 8.1 offers Powershell 4.0. Powershell 4.0 can be installed on Windows 8 without applying the 8.1 update. Powershell 4.0 requires at least .NET 4.5.

PowerShell has become so popular with administrators, pentesters, and hackers. PowerShell is:

- Native to Windows
- Able to call the Windows API
- Able to run commands without writing to the disk
- Able to avoid detection by Anti-virus
- Already flagged as "trusted" by most application whitelist solutions
- A medium used to write many open source Pentest toolkits
- Available on Linux builds (Ubuntu 14.04/16.04 and CentOS 7.1) and Mac OS X 10.11 or later[19]
- Able to administer local or remote systems

Windows Powershell has execution policies and can be restricted with user permissions, however the execution policy is not intended as a security control rather intended to prevent administrators from arbitrarily executing scripts. The default policy is *Restricted*, meaning no script, local, remote, or downloaded can be executed on the system. There are several ways to bypass, turn off, or override PowerShell's execution policies. Execution policy can be changed per session or globally on the system. There are four execution policies for PowerShell.[20]

- **Restricted** No Script either local, remote or downloaded can be executed on the system.
- **AllSigned** All script that are ran require to be digitally signed.
- **RemoteSigned** All remote scripts (UNC) or downloaded need to be signed.
- **Unrestricted** No signature for any type of script is required.

[19] https://github.com/powershell/powershell
[20] https://technet.microsoft.com/en-us/library/ee176961.aspx

SWGDE Windows 8 and 8.1 Tech Notes

History

Revision	Issue Date	Section	History
1.0 DRAFT	2016-09-15	All	Initial draft created and voted by SWGDE for release as a Draft for public Comment.
1.0 DRAFT	2016-10-08	All	Formatting and tech edit performed for release as a Draft for public Comment.
1.0	2017-01-12	None	Following period of Public Comment, no feedback was received and no edits were made. SWGDE voted to publish as an Approved document (Version 1.0).
1.0	2017-02-21	Formatting	Formatted and published as Approved Version 1.0.