Scientific Working Group on
Digital Evidence

SWGDE Technical Notes on Microsoft Vista

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 user's responsibility to ensure they have the most current version of this document. It is recommended that previous versions be archived for future reference, as needed, in accordance with that organization's policies.

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.

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

Table of Contents

1. Purpose

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

2. Overview of Vista

2.1 Versions

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

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

With the exception of Vista 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 128GB. All versions of Vista support 64 bit, but the user must register and request that a DVD be sent to them by Microsoft.

2.1.1 Vista 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 Vista Home Basic

This is the successor to Windows XP Home. Microsoft states that it is meant for the home or a small business network. It contains Internet Explorer 7, Windows Media Player 11, Windows Movie Maker, and Windows Mail (the successor to Outlook). It allows users to backup user files to a local disk or DVD. Automated indexing of the contents of the hard disk allows users to utilize instant searching.

2.1.3 Vista Home Premium

This is the successor to Windows XP Media Center, and it is what most OEMs are selling. It incorporates all of the options available in Home Basic. In addition, it offers the aero glass interface and Windows Media Center-type features including Movie Maker in hi definition and Media Center Extender (which allows the extension of Media Center to multiple devices). It includes Windows Meeting Space and support for Tablet PCs. It allows users to (1) backup user files to a local disk or DVD, (2) to schedule automated backup of user files, and (3) to backup user files to a network device.

2.1.4 Vista Business

This is the successor to Windows XP Professional. It breaks from the multimedia-heavy capabilities in Home Basic and Home Premium and instead focuses on the type of business features available in XP Pro: connecting to a corporate domain, encrypting files (EFS), Windows Meeting Space, host or client Remote Desktop, full Tablet PC features, roaming user profiles, and offline files and folders. Backup options include (1) backup of user files to a local disk or DVD, (2) scheduled automated backup of user files, (3) backup of user files to a network device, (4) use of the Windows PC Back Up and Restore function, and (5) use of Windows shadow copy.

2.1.5 Vista 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 Vista Business and adds BitLocker full volume encryption. The license allows the user to run up to four (4) additional copies of Vista using Virtual PC 2007. Backup options include (1) backup of user files to a local disk or DVD, (2) scheduled automated backup of user files, (3) backup of user files to a network device, (4) use of the Windows PC Back Up and Restore function, and (5) use of Windows shadow copy.

2.1.6 Vista Ultimate

This includes everything in Home Basic, Home Premium, Business, and Enterprise. It includes Windows Meeting Space, the encrypting file system, mobility center and Tablet support, Media Center and Media Center Extender, remote desktop, Windows DVD Maker, Movie Maker in hi definition, and BitLocker. Backup options include (1) backup of user files to a local disk or DVD, (2) scheduled automated backup of user files, (3) backup of user files to a network device, (4) use of the Windows PC Back Up and Restore function, and (5) use of Windows shadow copy.

* Preceding information from *Windows Vista Inside Out*, Ed Bott, Carl Siechert, and Craig Stinson, Microsoft Press, 2007.

2.2 Startup/Bootup

Vista's predecessors (NT, 2000, and XP) used a system based on the Windows NT boot loader, NTLDR, to boot up the operating system. Essentially, as the computer boots up, the NTLDR file, containing the main boot loader, loads from the hard drive's boot sector. Once NTLDR starts, it looks for hiberfil.sys and an active hibernation image. If NTLDR finds both the file and image, the operating system resumes from a hibernation state.

If an active hibernation image is not found, NTLDR reads the Boot.ini file, which contains special configuration options for booting the operating system as well as instructions for displaying the boot menu. If multiple configurations or versions of the operating system are available, NTLDR displays the list of boot entries to allow the user to specify which one should be loaded. Next, NTLDR launches Ntdetect.com, which is responsible for detecting the basic hardware that is necessary to start the operating system. Finally, NTLDR launches Ntoskrnl.exe, which is the kernel image for an NT-based operating system.

Vista dispenses with NTLDR and replaces it with a system built around three main components: a new boot loader architecture (Boot Manager + operating system loader + resume loader); a new boot option storage system called Boot Configuration Data (BCD); and a new boot option editing tool called BCDEdit.exe.

In this new system, as the computer boots up, the Boot Manager loads first and reads the Boot Configuration Data, which is essentially a database of configuration information stored on the hard disk in a format similar to the registry. When Boot Manager reads the Boot Configuration Data, it uses the information it finds in the database to determine if it needs to display its menu. If a menu is not necessary, Boot Manager does one of two things, depending on the information it finds in the Boot Configuration Data database: it passes control over to either the resume loader or the operating system loader.

If the Boot Configuration Data database contains information about a current hibernation image, Boot Manager passes that information over to the resume loader. Once that handover occurs, Boot Manager exits and the resume loader takes over. At this stage, the resume loader reads the hibernation image file and uses it return the operating system to the state it was in when hibernation was invoked.

If the Boot Configuration Data database doesn't contain information about a current hibernation image, Boot Manager retrieves boot configuration information and then passes that information over to the operating system loader. Once that handover occurs, Boot Manager exits and the operating system loader takes over. At this stage, the operating system loader loads the kernel, Ntoskrnl.exe, and any basic hardware drivers. As it does so, the Vista operating system boots up.

Although Vista’s boot system has changed dramatically, the Boot Configuration Data (BCD) is designed to handle systems with multiple versions and configurations of Windows, including versions earlier than Vista. It can also handle non-Windows operating systems. If Boot Manager finds information in the Boot Configuration Data database about another operating system, Boot Manager will build and display a menu that lists Vista and the other operating system as choices. If the other operating system is selected, Boot Manager retrieves information about how to boot that operating system and then passes the information over to the appropriate operating system loader. As stated above, Boot Manager then exits and the other operating system's boot loader takes over.

In pre-Vista systems, when a user wanted to edit the Boot.ini file, all that was required was opening the file in Notepad and making the appropriate edits. This is not true with BCD. Users can interact with BCD through several tools. The details of what can be modified depend on the particular tool, but BCDEdit.exe is the primary tool. You need administrative credentials to modify BCD.

BCDEdit.exe is a command-line utility that replaces Bootcfg.exe.   BCDEdit.exe is located in the \Windows\System32 directory of the Vista partition and is used to add, delete, and edit entries in the BCD store. If you prefer not to use a command-line tool, the free application

VistaBootPRO allows the user to modify the BCD in a GUI interface. VistaBootPRO is available for download at www.vistabootpro.org/index.php.

** The preceding information is from the following sources:

Get to Know Windows Vista's New Boot Loader Architecture, Greg Schultz, TechRepublic, *http://articles.techrepublic.com.com/5100-10877_11-6169638.html;*

Boot Configuration Data in Windows Vista, *www.microsoft.com/whdc/system/platform/firmware/bcd.mspx*.

*** See Registry section for more information about services startup and the registry entries regarding them.

2.3 Security

Because much of operating system, including its networking technologies, has been redesigned and new code written, Vista is likely to present some vulnerabilities that weren't in older versions of the OS even as it fixes many that were. Vista includes a number of new security enhancements that XP doesn't have. For example, User Account Control (UAC) in Vista protects against attacks that rely on elevation of privileges. As in XP, a user's first account will be as Administrator; however, the User Access Control feature requires permission from the user before "true" Administrator activity is required (such as installing new applications). Internet Explorer 7, when running on Vista, leverages UAC to run in Protected Mode, which keeps Web applications from writing to system folders. IE7 doesn't run in Protected Mode on XP.

BitLocker drive encryption, available in Vista Enterprise and Ultimate versions, provides a way to keep unauthorized persons from accessing sensitive data on a stolen or lost laptop. The Windows Firewall in Vista allows you to block outgoing traffic as well as incoming. Windows service hardening reduces the potential for damage if one of Windows' services is compromised. Vista includes the Network Access Protection client, which allows administrators to restrict computers that are properly updated or don't have antivirus, anti-spyware, or firewalls from connecting to company networks.

2.4 File System: Major Changes and Additions

From concept, Vista was supposed to have included Microsoft's new WinFS (Windows Future Storage) file system – a file storage subsystem that runs on NTFS and uses SQL Server-related technology to create sophisticated indexes of a wide variety of data. But support for it in Vista was dropped so that Vista could ship in a reasonable timeframe. WinFS may be added to Vista in future versions.

Vista still uses the NTFS file system used in XP. The file structure has been changed, but not the file system. Most of the changes come under the old Documents and Settings location; in essence, the "My" has been removed from the beginning of each directory (ex. "My Documents" has become "Documents"). Legacy paths are reparse points (shortcuts) to the new location and are hidden from the user by default; they are generally only used by applications that are "looking" for that directory. In addition, the reparse points are protected so that normal users cannot use them; instead, users must use the current paths.

Microsoft's changes to NTFS for Vista include WinFS-like features such as support for metadata and advanced searching. The changes allow for the initial move away from the customary drive and directory storage model, or location based file storage, that we all know and more toward a metatag-driven search.

Large, voluminous files and numerous documents are untethered from the hierarchical file structures of earlier Windows versions by indexing filenames, metatags, and even file content. Files and folders can easily be virtually grouped together based on a variety of criteria without the need to drag and drop them into various folders. With the addition of enhanced indexing capability, the physical location of a file/folder ceases to be an issue for users.

2.4.1 Partition Table

Vista allows for use of GUIDS (global unique identifiers) in the partition table. This change is transparent to the user and instead may be used for future software development. It is not activated by default.

2.4.2 Starting Sector Change

The first NTFS partition starts at sector 2048, not sector 63. This new address allows for better alignment of partitions.

Transaction NTFS (see section below for more specific information)

2.4.3 Time and Date Stamps

In an attempt to increase performance in Vista, the file system no longer records Last Access information; it is disabled by default. Vista will populate the Last Access date and time with the File Creation date and time. Examiners should not rely on the Last Access date and time. Examiners may want to check the Registry key for the Last Access time on in Vista at

HKEY_LOCAL-MACHINE\SYSTEM\CurrentControlSet\Control\FileSystem\"NtfsDisableLastAccessUpdate"

("0" means Last Accessed date and time is being recorded, "1" means no recording). The default key setting is "1."

2.4.4 Default File and Folder Locations

Most of the changes come under the old Documents and Settings location. Legacy paths are reparse points to the new location and are hidden from the user by default. They are also restricted so that normal users cannot use them; they are generally used by applications "looking" for those directories. A User's directory path contains:

- Contacts,
- Desktop,
- Documents,
- Downloads,
- Favorites,
- Links,

- Music,
- Pictures,
- Saved Games,
- Searches,
- Videos.

"AppData" is the new version of "Application Data" from XP, and most information about usage is located here (Internet Explorer, History, temporary internet files).**Windows Mail** has replaced Outlook Express. Email messages are stored as individual files rather than a binary database. (See Appendix A)

2.4.5 Disk Defragmentation

All system and data drives and volumes will be automatically defragged. This defragmentation is scheduled by default in Vista for 3AM local time every Wednesday. If the machine is off at that time, it will not defrag at startup.

2.4.6 Virtual Registry and Registry Transaction Logging (TxR)

This is the representation of certain portions of the Registry housed in the user's profile. If Vista does not have access to the write to the Registry (ex. when the user is running a virtual machine), the writes will be made to a log contained in the user's profile.

2.4.7 Prefetch/Superfetch

The term "prefetch" is sometimes used interchangeably by Microsoft with the term "superfetch." Prefetching is used as performance optimization technology to allow for faster boot time and fast application loads. Prefetch is enabled by default for boot and applications. During disk optimization, Vista calls on the layout.ini file in the Prefetch directory and tries to clear enough space on the outside of the platter to move prefetch files in a continuous sequence from most frequently run to least frequently run). This is a limited defragmentation that runs roughly every three (3) days.

Prefetch files must be translated and viewed using a hex editor. Vista will create prefetch files of the last 128 user-run applications. These prefetch files also include the number of times the application is run (start counting at 5) and the last time the application is run.

Boot prefetch info is contained in a special file in the Prefetch directory called NTOSBOOT-B00DFAAD.pf (typically the largest file in Prefetch directory). The naming convention for prefetch files is binary name, hex representation to path of file, prefetch file extension (ex. NOTEPAD.EXE-AF172368176328.PF). Using a hex editor, you will see the name of the application at offset 16(d)/10(h). The last execution time is an 8-byte value starting at 128(d)/78(h). The number of times the application has been run is a 4-byte value starting at offset 152(d)/90(h).

2.4.8 Event Logs and Formats

Logging is sent to "event channels" that can be secured; more than one machine can listen to a channel. Data from event channels are archived in event logs, which are a proprietary format. Vista uses HTTP or HTTPS to send events to a channel. A channel is a named stream of events (think of a TV channel) that is intended for specific audiences.

Event logs are stored in schematized binary XML (which allows for inclusion in an SQL database); these logs are not easily readable. Logs are stored at:

%SystemRoot%\system32\winevt\Logs.

Windows Events Command Line Utility (WEvtUtil.exe) enables the retrieval of info about event. It retrieves information about logs and publishers, install and uninstall event manifests, run queries, and export/archive/clear logs (primarily focused on live events and logs). The Microsoft Log Parser tool doesn't currently support parsing .evtx files; the best method of viewing logs is in the Event Viewer utility.

2.4.9 Volume Shadow Copies

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. This can also be called Volume Shadow Copy Service or Volume Snapshot Service (VSS). VSS monitors the system by default and records ALL changes on the disk during snapshot creation. VSS pauses all write access to the disk (for a maximum of 60 seconds) during the initial stages of the backup, which allows for the backup of even files that are currently in use. If a file is changed multiple times between snapshots, only the most recent change will be recorded in the current snapshot. VSS can be differentiated from System Restore because System Restore only tracks changes to applications and the system (i.e. non-user files).

There are two methods for creating a volume shadow copy: clone or plex (full copy of original data on a separate volume) or copy-on-write (differential copy where only changes are stored).

In Vista Business and higher, the Control Panel contains "Backup and Restore Center" which allows the user to choose to backup files or backup computer.

2.4.10 Recycle Bin

It comprises approximately 7% of the drive space. The \Recycled or \Recycler folders have been replaced with \$Recycle.Bin at the root of the volume.   It is still defined per user and per drive. 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 When a $I file is created, the file creation date and time is the same as the file deletion time and date. At offset 16(d)/10(h) is the 8-byte date and time that the file has been created for each $I entry. The file path name for $I file begins at offset 24(d).

2.4.11 Thumbs.db

Thumbs.db is now gone. It has been replaced with a centralized thumbnail caching feature (called thumbcache), stored PER USER PROFILE at:

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

Thumbnails from removable or network media are also stored in the same directory. Four database files are located in the profile—these relate to the resolution of the thumbs:

1. Thumbcache_1024.db
2. Thumbcache_256.db
3. Thumbcache_96.db
4. Thumbcache_32.db

In a change from XP, the Vista Disk Cleanup function will by default clear thumbcache. This is just a delete, not an overwrite. A system-wide policy can be set to never store thumbs using the Folder Option menu in Explorer; this setting will show icons, not thumbnails. This setting is not on by default.

2.4.12 Internet Explorer V7

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:As in XP, Examiners can still access Typed URLs at HKEY_USERS\<GUID>\Software\Microsoft\Internet Explorer\TypedURLS. The setting to allow pop-ups is HKEY_USERS\<GUID>\Software\Microsoft\InternetExplorer\New window\Allow.

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

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

There will be a \Low directory under the user's profile as well because IE runs at a lower process level than the user herself. Since it can't write to the operating system itself, it writes to this folder. Browsing to a site that is in a more trusted zone from the normal security prompts the user to open a new browser window in a new tab. This results in the same instance of IE running with multiple tabs.

RSS feeds will be stored as:

- %userprofile%\AppData\Local\Microsoft\Feeds.

The INDEX.DAT file is now overwritten in IE7 in Vista, not just deleted. However, with volume shadow copies, the Examiner may be able to reconstruct at least some of this data.

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

2.4.13 Address Space Layout Randomization

Windows Vista incorporates Address Space Layout Randomization (ASLR) in memory. The goal of ASLR is to make it hard to predict where the operating system functionally resides in memory. What this means for a computer forensic examiner is that whenever a Vista computer is rebooted, ASLR randomly assigns executable images such as DLLs and EXEs to one of 256 possible locations in memory. Therefore, any examinations that seek information at specific memory addresses may not be successful.

2.5 Registry

Please note that at this time, current research indicates that no forensically significant changes to the Vista Registry have been identified. However, a number of new functionalities may impact Registry entries.

Microsoft VISTA registry provides a service called, “User Account Control.” What this provides is the ability to give administrators the option of restricting permissions while still allowing most applications to run.

A system of File and Registry Virtualization allows for this combination of security and compatibility. This file and registry virtualization automatically redirects writes and the subsequent reads to reserved areas that the standard user would not have access to.

When the changes are made, these changes to the virtual registry settings and folders are exclusive to only the affected user account and the affiliated applications that the user runs, thereby maintaining the integrity of the computer as a whole. When Administrator credentials are required to execute an application, Windows Vista will prompt the user for these credentials prior to executing the application.

From a forensic standpoint, there are many legacy Windows applications that have been created which allowed access to parts of the file system and registry. These areas are now locked by Windows Vista. Microsoft has developed a process, within Windows Vista, that allows for backward compatibility. This should allow this legacy software to still work. This will be accomplished by incorporating the UAC virtualization services referenced above. Read-write operations are made from the protected portions of the file system and registry to unprotected user specific locations. The entire process will appear to be transparent to legacy software and will occur automatically. (See Appendix B)

2.6 Encryption

Keeps data confidential through full-volume encryption and boot-integrity monitoring.

2.6.1 BitLocker

BitLocker Drive Encryption is a hardware-enabled data protection feature in Windows Vista Enterprise or Ultimate that helps protect data. By encrypting the entire Windows volume, it prevents unauthorized users from accessing data by breaking Windows file and system protections or attempting the offline viewing of information on the secured drive. Due to these restrictions, examiners may want to consider obtaining two (2) forensic images of a live system running BitLocker: a logical image and a physical image. How the user is signed in (Administrator or at a lower permission level) may affect what types of files will be included in the logical image. In any event, the examiner should document any and all actions taken during a live acquisition.

BitLocker enables secure and easy recovery by an authorized administrator. It uses the Trusted Platform Module (TPM) version 1.2 chip incorporated on the computer's motherboard or higher or a USB device for secure encryption key protection and to measure and test key components as the computer is booting up. The system and hardware integrity are checked early in the machine boot process, and the computer will not boot if system files or data have been tampered with. BitLocker features centralized storage and management of encryption keys in Windows Active Directory®, and it also allows IT administrators to store encryption keys and restore passwords onto a USB key or to a separate file for additional backup. BitLocker provides for system recovery even "in the field." A user who needs to use BitLocker's recovery mode can simply enter a recovery password, and Windows operation will continue normally.

BitLocker also offers the option to lock the normal boot process until the user supplies a PIN code or inserts a USB flash drive that contains the appropriate decryption keys. These additional security measures provide multifactor authentication and assurance that the computer will not boot or resume from hibernation until the correct PIN or USB flash drive is presented.

BitLocker requires at least two (2) NTFS formatted partitions, one at least a 1.5GB system partition, and one any size Windows boot partition. There are three (3) phases to a Vista install compatible with BitLocker: drive preparation, operation system installation, and enabling of BitLocker and volume encryption.

There are several items of note regarding BitLocker. There are currently no third party tools for decrypting a BitLocker volume. Also, all user and system files are encrypted including the swap and hibernation files. There are at least two (2) methods (of varying intrusiveness) for determining whether BitLocker is running on a computer. **both methods require Administrator Privileges to run**:

1. At the Start button, search for "bit"; click on the presented icon and open the BitLocker management window
2. From a command prompt, navigate to the system32 directory and type in cscript manage–bde.wsf –status, which returns an encryption report on the drive(s)

Recovery Mode requires a 48-digit recovery password/key either stored on a USB Flash Drive or entered via the function keys (ex. F1=1,…, F10=0). Using the future Secure Online Key Backup service (i.e. MS Windows Digital Locker), a user can store a Recovery Password on the Digital Locker website and thus retrieve it from any computer that accesses the internet. In enterprise environments, the BitLocker encryption key will typically be escrowed on the server. In any event, appropriate administrative or judicial process may be required in order to access the encryption key.

There are two BitLocker tools of possible use, **but note that each of them requires that the user has the original BitLocker password or the 48-number recovery password:** BitLocker Repair and BitLocker RP Viewer for Active Directory. BitLocker Repair recovers data from a damaged drive. BitLocker RP Viewer for Active Direcotry is a free tool from Microsoft, used in an enterprise environment, that allows the user to search the network by computer name, computer drive label, or password ID.

2.6.2 Encrypted File System

The Encrypting File System (EFS) is a core encryption technology that enables you to encrypt files stored on NTFS volumes. Examiners are accustomed to EFS since it is integrated with the NTFS file system. Users select the files to be encrypted, but users do not have to manually decrypt files before use—they can simply open and change a file as they would normally. Windows Vista uses version 3 of the $EFS stream. Windows XP and Windows Server 2003 use version 2. Windows Vista updates the $EFS stream on encrypted files to version 3. There is currently no option to save EFS-encrypted file in Windows Vista by using a format that can be opened in windows XP or in Windows Server 2003.

With Windows Vista, as in XP, the encrypted files are protected even if an attacker gains physical possession of the computer. In addition to encrypting the selected files, Vista also has the ability to encrypt the System page Files.

In Windows Vista, EFS supports storing user keys as well as administrative recovery keys on smart cards. If smart cards are used for logon, EFS operates in a Single Sign On mode, where it uses the logon smart card for file encryption without further prompting for the PIN.

EFS in Windows Vista can also be used to encrypt the system page file. This feature can be enabled by the administrator through Group Policy. The Client Side Cache, which stores offline copies of files from remote servers, can also be encrypted with EFS. When this option is enabled, files in the cache are encrypted to specific users, and even local administrators cannot read them without having access to the users' private keys. EFS will be available in the Windows Vista Business, Enterprise and Ultimate editions.

As in XP, System Restore will not backup EFS encrypted files. Vista PC Backup and Restore will not backup EFS encrypted files.

**** The preceding information is from:

http://technet2.microsoft.com/WindowsVista/en/library/c61f2a12-8ae6-4957-b031-97b4d762cf311033.mspx?mfr=true

2.7 Windows Live/Live Messenger

Windows Live is the collective brand name for a set of services and software products from Microsoft. A majority of these services are Web applications, accessible from a browser, but there are applications that need installing as well. There are three basic groups of these services: informed, connected and protected experiences.

2.8 Windows Defender

Windows Defender, previously known as **Microsoft AntiSpyware**, is a software product from Microsoft designed to prevent, remove and quarantine spyware in Microsoft Windows. It is part of Windows Vista and available as a free download for Windows XP and Windows Server 2003.

3. Acquisition

Since the security features are more robust in Vista, then access to data after a target machine is powered down may be quite difficult.

When responding to systems that are currently powered down, current "best Practices" should continued to be followed.

When responding to a live system and prior to acquisition, serious consideration should be given to the following:

- Identification of Operating System
- Volatile Data Collection
- Imaging of RAM
- Documentation of open ports and running processes
- Users logged in
- Presence of encrypted disks or volumes

***** *For information regarding live acquisitions, refer to SWGDE document on Live Acquisition of Computer Systems.*

4. Processing

Other than bitlocker and EFS encryption, there are no differences in the forensic processing of Vista over other Windows based systems.

5. Glossary

Bitlocker: An operating system-level extension to Vista that combines on-disk encryption and special key management techniques. The data and the operating system installation are both protected by two-factor authentication, specifically, a hardware key used in conjunction with a long passphrase.

Volume Shadow Copy: Allows taking manual or automatic backup copies or snapshots of a file or folder on a specific volume at a specific point in time.

6. Resources

http://www.microsoft.com/windows/products/windowsvista/features/default.msp/ (New Vista features)

http://msdn2.microsoft.com/en-us/library/aa365680.aspx

http://www.symantec.com/avcenter/reference/Windows_Vista_Security_Model_Analysis.pdf

http://www.microsoft.com/technet/windowsvista/security/guide.mspx

Daylight savings time help and support center

http://support.microsoft.com/default.aspx/gp/cp_dst

BitLocker Resources: BitLocker Homepage:

http://www.microsoft.com/technet/windowsvista/security/BitLocker.mspx

Appendix A: XP vs. ***Vista (IN BOLD)*** File Path Comparison

\Documents and settings\
\Users\\

\Documents and settings\All Users\
\ProgramData\\

\Documents and settings\All Users\Start Menu\
\ProgramData\Microsoft\Windows\Start Menu\\

\Documents and settings\All Users\Application data\
\ProgramData\\

\Documents and settings\All Users\Desktop\
\Users\Public\Desktop\\

\Documents and settings\All Users\Documents\
\Users\Public\Documents\\

\Documents and settings\All Users\Documents\My Pictures\
\Users\Public\Pictures\\

\Documents and settings\All Users\Documents\My Videos\
\Users\Public\Videos\\

\Documents and settings\All Users\Documents\My Music\
\Users\Public\Music\\

\Documents and settings\All Users\Favorites\
\Users\Public\Favorites\\

\Documents and settings\Default User\
\Users\Default\\

\Documents and settings\Default User\Local settings\History\
\Users\Default\AppData\Local\Microsoft\Windows\History\\

\Documents and settings\Default User\Cookies\
\Users\Default\AppData\Roaming\Microsoft\Windows\Cookies\\

\Documents and settings\Default User\Recent\
\Users\Default\AppData\Roaming\Microsoft\Windows\Recent\

\Documents and settings\Default User\SendTo\
\Users\Default\AppData\Roaming\Microsoft\Windows\S endTo

\Documents and settings\Default User\Start Menu\
\Users\Default\AppData\Roaming\Microsoft\Windows\S tart Menu

\Documents and settings\Default User\Local settings\Temporary Internet Files\
\Users\Default\AppData\Local\Microsoft\Windows\Tem porary Internet Files

\Documents and settings\Default User\Local settings\Application data\
\Users\Default\AppData\Local\

\Documents and settings\Default User\Local settings\
\Users\Default\AppData\Local\

\Documents and settings\Default User\My Files\
\Users\Default\Documents\

\Documents and settings\Default User\My Files\My Music\
\Users\Default\Music\

\Documents and settings\Default User\My Files\My Pictures\
\Users\Default\Pictures\

\Documents and settings\Default User\My Files\My Videos\
\Users\Default\Videos\

\Documents and settings\Default User\Application data\
\Users\Default\AppData\Roaming\

> ****** File paths that include 'Default User' could be replaced by any users name, used on both sides (e.g. \Documents and settings**<users name>**\My Files\My Videos\ would then be ***\Users\<users name>\Videos\***)

Appendix B: Registry

The Windows Registry is a hierarchical database that acts as a central repository for system configuration data. It stores most of the settings within Windows and is heavily utilized by third party software and hardware vendors.

Since the release of Windows 2000 there are five (default) registry hive files: Default, SAM, Security, Software and System – which are located in the path \Windows\System32\Config (same place as the event log files). These files can not be opened while the system is running. (Older Windows systems, "legacy" systems, have different files which make us the registry information and which are located in different paths.)

The structure of the Windows Registry is similar to the Windows File System:

- hives are the "on disk" representation of the registry information
- keys are the "folders" that store other keys and values
- Values are the containers that store actual data
- types define the format for data stored in the value – there are 15 different types but the vast majority are REG_DWORD, REG_SZ , REG_LINK and REG_BINARY

There are five root level keys:

1. HKEY_CLASSES_ROOT (HKCR)
2. HKEY_CURRENT_USER (HKCU)
3. HKEY_LOCAL_MACHINE (HKLM)
4. HKEY_USERS (HKU)
5. HKEY_CURRENT_CONFIG (HKCC)

Of these five, the most important are HKLM and HKU as they are the only keys that Windows stores on the disk. The remaining keys are actually virtual representations of values that already exist under one, or combination of both, of those two keys:

HKEY_CLASSES_ROOT - Virtual merging of HKLM\Software\Classes and HKCU\Software\Classes – it contains file associations, and class name and GUID of registered component objects. This can contain useful indications of types of programs that were installed at one time on the machine.

HKEY_CURRENT_CONFIG – is a link to the data for the current hardware profile from the key HKLM\SYSTEM\CurrentControlSet\Hardware\Profiles\Current. In turn, Current is a link to the key HKLM\SYSTEM\CurrentControlSet\Hardware\Profiles\nnnn, where nnnn is an incremental number beginning with 0000.

HKEY_USERS – Contains a listing of all users on the system by GUID (Global Unique Identification) number. Each users settings are listed here and linked to the HKEY_CURRENT_USER hive when that user logs into the system.

- .Default – maps to the DEFAULT hive – a profile that the system uses when no users are logged on
- S-1-5-18, S-1-5-18.Classes, S-1-5-19 etc – SID of local user account
- S-<long series of numbers> - SID of Domain user account

HKEY_CURRENT_USER – a link to the logged on users' section of the registry under the HKEY_USER hive. All settings for a particular user are mapped to/from this hive.

HKEY_LOCAL_MACHINE – Configuration information for the computer and is the home of the five subkeys Hardware, SAM, Security, Software, and System.

- HKLM\Software – contains software configuration information. Installed applications write settings here and typically use the software manufacturer name. It's also used for OS settings under HKLM\Software\Microsoft\Windows and Windows NT
- HKLM\System – Contains system level configuration options, startup parameters and installed services. Subkey CurrentControlSet is a virtual map of either ControlSet001 or ControlSet003. Which set being used is determined by HKLM\System\Select\Current.

There are no MAC date/time values for the registry entries, but each registry key contains a LastWrite Time value. If the key is changed or a value within that key is changed then the time is updated for the entire key. These times cannot be viewed with the systems RegEdit tools, but you can print a section to expose the data. Numerous commercial tools do expose these values however.

The following table shows some important basic system information that can be found in the registry, and the key it can be found in:

What	Where
System version and related info	HKLM\Software\Microsoft\Windows NT\CurrentVersion
System install date Note that the value is listed in seconds measured from 12:00am Jan 1, 1970. There are a number of decoding tools available.	HKLM\Software\Microsoft\Windows NT\CurrentVersion
Registered Owner Name provided by user during install	HKLM\Software\Microsoft\Windows NT\CurrentVersion
Registered Organization Provided by user during install	HKLM\Software\Microsoft\Windows NT\CurrentVersion

What	Where
Computer Name Numerous entries for this throughout the registry	HKLM\SYSTEM\<ControlSetnnnn>\ Services\EventLog\Computer Name
Start Locations Services and drivers that are loaded at startup and login time	HKLM\Software\Microsoft\Windows\ CurrentVersion\Run HKCU\Software\Microsoft\Windows\ CurrentVersion\Run HKLM\Software\Microsoft\Windows\ CurrentVersion\RunOnce HKCU\Software\Microsoft\Windows\ CurrentVersion\RunOnce HKLM\Software\Microsoft\Windows\ CurrentVersion\RunServices HKLM\Software\Microsoft\Windows\ CurrentVersion\RunServicesOnce HKLM\Software\Microsoft\Windows\ CurrentVersion\RunOnce\Setup

It is important to note that many of the values listed above can be modified and changed over time. These changes can be tracked through a number of ways by looking at stored registry and log file based resources (example, restore points).

Note about services. Looking at the entries in HKLM\SYSTEM\CCSnnn\Services displays services running on the system. These services can also be displayed using the command line utility SC.EXE. When combating the Malware defense, it is important to look here to investigate each service to make sure that each should be there, that they start as expected, that their path is legitimate, etc. Default settings for services can be found at

www.microsoft.com/resources/documentation/windows/xp/all/proddocs/en-us/sys_srv_default_settings.mspx.

Additionally, the Registry contains a number of locations that are referenced with the system starts and when a user logs on. The most popular are the Run and RunOnce registry locations. For more information see http://support.microsoft.com/kb/179365

History
SWGDE Technical Notes on Windows Vista

Rev #	Issue Date	Section	History
1.0	02/08/2008	All	Initial Issue