

A Framework for Computer Forensics Investigations Involving Microsoft Vista

Darren R. Hayes and Shareq Qureshi, *Pace University*

Abstract-The technical environment continues to change and impact the work of digital investigations. This research provides a framework within which computer forensics investigators can take advantage of new or different types of evidence from Microsoft's Vista operating system ("Vista"). Moreover, this paper will also indicate the many challenges that investigators will encounter when faced with the Vista platform. The focus herein will be on changes associated with new security, encryption and file restoration features. These features vary according to the version of Vista and these differences will also be discussed. This research will also detail the integrity of data recovery procedures through detailed experiments used to identify how data could be manipulated by a perpetrator in Vista as compared to previous versions of Microsoft's operating systems. Ultimately, this paper will indicate that enhancements in security and encryption associated with Encrypted File System (EFS) as well as BitLocker Drive Encryption are very problematic for investigators. Vista has serious implications for computer forensics investigations. Nevertheless, this research will guide the digital investigator through the labyrinth of new challenges, to effect a more thorough investigation of digital evidence.

Index Terms-Vista, BitLocker, Encryption, Operating Systems, Computer Forensics, Computer Security.

I. INTRODUCTION

Windows Vista is a dramatic departure from previous versions of Microsoft's operating systems. The changes to this operating system are primarily in the area of security, which is of great importance to the computer forensics examiner. Microsoft clearly understands that not all users are the same. The younger generations, who spend numerous hours on the Internet, using multimedia devices are also keen social networkers. Then there are the Baby Boomers who are technically-savvy. There are also a growing number of senior citizens utilizing the Internet and computers in general. Microsoft has therefore created varying levels of access, referred to as User Access Control.

Vista has broached the continually changing nature of malware threats from the Internet as well as their frequency. Vista programs like *Windows Defender* and the corresponding *Windows Live OneCare* demonstrates that Microsoft understands that the average user cannot bear the entire burden of protecting a system from threats and thus the operating system has assumed more security responsibilities. Data protection was clearly an important initiative for Microsoft when developing Vista. BitLocker Drive Encryption that utilizes Trusted Platform Module, Encrypted File System and e-mail encryption in Windows Mail are very different features from what existed previously in Microsoft operating systems.

This paper does not describe every possible change that affects forensic examinations but rather it covers the most common areas that an examiner will encounter. The paper explains what effect a particular Vista feature may have on conducting a forensic examination. Indeed, this research addresses the changes in the operating system's structure, including encryption, Windows registry, event logs, windows Search Engine (indexing), Windows mail, Windows firewall, file restoration, file system, hiding files in slack and Bitlocker. The comparisons made herein are, for the most part, between Vista and XP or previous versions of Microsoft operating systems.

II. WINDOWS VISTA – SECURITY, ENCRYPTION & FILE RESTORATION

This paper will focus on changes in Vista which will likely have the greatest impact on computer forensic investigations starting with the built-in encryption and backup features. Before doing so, though, it is necessary to take a quick look at the numerous versions of Vista available. Accurate identification of the specific version of an operating system is always important during an investigation. With the 32-bit and 64-bit versions of Vista it is more crucial than ever because different features with important implications for examiners, are available, most notably perhaps the inclusion of backup and encryption facilities.

Forensic professionals should note the following table below, which illustrates that the security features of Vista vary based on the edition:

The proceeding section will focus on the features of these different versions and what implications they may have for investigators [12].

A. BitLocker Drive Encryption

Initially there may have been concerns within the computer forensics community that the proposed encryption features of Vista, especially BitLocker, would result in a huge increase in the amount of encrypted data confronting examiners. However, it is now clear that these features will be limited to the higher end editions of Vista only and are not implemented by default. Nevertheless, BitLocker continues to intriguing.

What exactly is BitLocker? Basically, BitLocker provides AES encryption of all data on a Vista volume, combined with integrity checking of the boot process, used to load the OS. The primary purpose of these features is to protect data, even if an attacker manages to circumvent the operating system or remove the hardware storage device. It should be noted that volume encryption is not new. Other software offering similar features are available and have been for some time. However, something which sets BitLocker apart from other encryption packages is its use of the Trusted Platform Module ("TPM 1.2"). A TPM can be summarized very briefly as a microcontroller, which securely stores data used in cryptographic or security processes (e.g. keys, digital certificates and passwords) with the aim of increasing the security of certain applications and features. When using a TPM chip to provide added security, BitLocker can be configured to either boot the system on completion of a successful integrity check of the boot files or (in theory at least) to require the entry of a PIN or USB device containing a startup key. BitLocker can also operate without TPM support through the use of a key located on a USB device inserted at system startup. Whatever the case, examiners need to be aware of the implications for what may need to be searched for and collected when a BitLocker system is seized (e.g. motherboard, USB drive, recovery key/password etc.) [12].

What are the implications of BitLocker for forensic examiners? In a recent Cyberspeak podcast, Jesse Kornblum spoke in some detail about the impact of BitLocker and the growth in importance of memory analysis for first responders [8]. The implication of this new change to Vista is that now may be the time when memory capture (and subsequent analysis) becomes the accepted norm for forensic examiners when first approaching a suspect's machine rather than the more traditional option of "pulling the plug". Developers of Helix, renowned for its live acquisition capabilities, would perhaps concur. Undoubtedly, BitLocker presents a challenge after all; one

of Microsoft's goals with BitLocker is to protect data even when the storage device has been removed from the user's physical control, a scenario not entirely dissimilar to lawful seizure. However, as BitLocker is only available in Enterprise and Ultimate editions of Vista and needs to be purposefully enabled on an appropriately formatted drive not to mention the hardware requirements for TPM. One should also remember that even where BitLocker is in use, the specific circumstances of the investigation, such as the ability to seize appropriate hardware or gain access to the volume by initiating a recovery procedure, mean that evidence may still be recovered in a straightforward fashion. Certainly the stakes have changed and the bar has been raised, but while BitLocker certainly represents a step towards more powerful and ubiquitous encryption it seems unlikely that its inclusion represents the watershed moment that some had feared [4].

B. Encrypting File System (EFS)

EFS is a feature available in the Business, Enterprise, and Ultimate editions of Windows Vista and provide file and folder level encryption on NTFS volumes (using the AES algorithm). In comparison with the hardware and setup requirements of BitLocker, EFS simply requires a checkbox to be ticked in the file or for the folder's properties to be enabled [11]. However, in larger environments, the encryption might be more likely to be set through Group Policies or scripting rather than by individual users [3]. EFS is not new - it can also be found in 2000, XP and Server 2003, and therefore would not appear to provide forensic examiners with a radically new challenge (one new feature to note in Vista's implementation of EFS, however, is that encryption certificates can now be stored on smart cards). As with BitLocker, or indeed any other form of encryption, live response and the use of standard recovery procedures - especially at the enterprise level - are likely to be key components of any plan to analyze encrypted data [4].

C. Backup and Restore

In contrast to encryption, some new features can actually work to the forensic examiner's advantage. One example is the increased prevalence of backup, which restores functionality within Vista. "The Backup and Restore Center" is a GUI-based wizard, available in the Home Premium, Business, Ultimate, and Enterprise editions of Vista, which enables users to schedule automatic backups of selected files (as well as providing a method for recovery). Generally speaking, users (especially home and small office users) are incredibly poor at backing up their data and where they do take the necessary steps to do so they are inconsistent at best, often backing up once and then forgetting to do so again for months at a time. The automatic scheduling component of "The Backup and Restore Center" should increase the chances of recent

backups being available for examiners. Backups can be created on external media as well so investigators should, as always, take into account the presence of DVDs, CDs, external hard drives and so forth when securing a scene. Another feature called "Complete PC Backup and Restore" is available in the Business, Ultimate, and Enterprise editions only and functions as a disaster recovery tool.

D. Shadow Copy, System Protection and Previous Version

Shadow Copy functionality automatically creates daily copies of files and folders with a view to maintaining system integrity (Shadow Copies can also be created manually by setting a "restore point"). As previously seen in Windows Server 2003, this functionality is now available in the Business, Enterprise, and Ultimate editions of Vista [12]. Of note for forensic practitioners is that, unlike other recovery features such as "Backup and Restore", the automatic creation of shadow copies is enabled by default (although it needs to be explicitly enabled for external volumes) and shadow copies are held locally. The default setting reserves 15% of a volume's disk space for shadow copies. It should also be noted that the system works by saving only incremental changes rather than full copies of files or folder. Shadow copy functionality is administered via the System Protection tab (*Control Panel -> System Properties*) and can be utilized by right clicking a file or folder within Windows Explorer and selecting "Restore previous versions". Similar types of "snapshot" functionality have existed in previous Windows operating systems to some degree but Vista's implementation represents a greater push by Microsoft towards encouraging its use by the end user rather than just applications or system administrators.

Available in the Home Premium, Business, Ultimate and Enterprise editions of Vista, "Scheduled and Network Backup" is a feature which does exactly what you might expect and allows backups to be made at regular, pre-defined intervals. This is handy for the user but even handier for the investigator examining the user's data and past activity.

E. File System

Detailed, comprehensive information from Microsoft about all of the changes implemented in Vista's file system are difficult to find, with perhaps the most obvious improvement offered at a lower level being Transactional NTFS (TxF). This feature allows a series of file system operations (collectively termed a "transaction") either to be carried out in its entirety or rolled back. Although this may be beneficial for system integrity it would not appear to have immediate significance from an investigative standpoint. Several operating systems provide a central logging service, which collect event messages from the kernel and applications, filters them and writes them into

log files. For more than a decade, this system service has existed in Microsoft Windows NT. Its file format is supported by most forensic software. Vista introduced an event logging service which had an entirely new design [6].

Forensic examiners are now confronted with unfamiliar system behavior and a widely undocumented file format. Log files belong to some of the most important sources of forensic evidence because they usually connect a certain event to a point in time. Major operating systems like UNIX or Microsoft Windows provide system-wide services to collect process and store event messages [3].

Encrypting File System (EFS) is a feature of Windows that allows the user to store information on his hard disk in an encrypted format. Encryption is the strongest protection that Windows provides to keep the information secure.

Some key features of EFS are:

- Encryption is simple; just select a check box in the file or folder's properties to turn it on.
- One has control over who can read the files.
- Files are encrypted when they are closed, but are automatically ready to use when someone opens them.
- If someone changes his mind about having a file encrypted, clear the check box in the file's properties.

EFS is not fully supported on Windows Vista Starter, Windows Vista Home Basic, and Windows Vista Home Premium. For those aforementioned editions of Windows, if someone has the encryption key or certificate, they can decrypt files, by running *Cipher.exe* in the command prompt window (advanced users), modify an encrypted file and copy an encrypted file as decrypted to a hard disk on the computer. Import EFS certificates and keys. They are also back up EFS certificates and keys by running *Cipher.exe* in the command prompt window.

F. Defragmentation and Restore

Windows Vista's *Disk Defragmenter* is configured to run on a regular schedule right out of the box. When it runs, it is hidden in the background with no visible interface or icon. This is a marvelous improvement because disk fragmentation can take a huge toll on the overall performance of your operating system. It can be the source of long boot-times, random crashes, and unexplained lock-ups. In fact, an extremely fragmented hard disk can even prevent a system from booting up. Defragmentation is the process of reorganizing a computer's "filing cabinet" and is designed to make the computer run more efficiently by putting pieces of files as close to each other as possible. Defragmenting a computer will not harm the active data (the data that users accesses on their own desktop) but may render a great deal of the normally recoverable deleted data (the data only a forensic engineer can recover) virtually unrecoverable. Depending on the size the drive, data volume and order of operations, deleted files might be recoverable even after defragmentation. A complete

computer forensic investigation will help identify data that is recoverable after defragmentation [12].

Experienced computer forensic investigators often are able to find bits and pieces of files left on the computer. Even more damaging, investigators frequently uncover evidence of the program itself as well as the date and time the program was used on the computer. When evidence of data destruction is apparent, the results of a thorough forensic examination will help attorneys and their client's best assess the merits of the case [9]. Restore points may contain the key piece of evidence to support a case, but are commonly overlooked. Content within restore points can be an incriminating piece of evidence against the defendant, exposing code, configurations and log files. Many times, these files can be found even after attempts at counter forensics such as log wiping, time/date stamping and secure deletion.

G. Hiding files in slack

Information attached to a file, such as a file header and metadata, are not technically separate files, but can be culled from the file as separate data objects. Other types of information found on storage media are not files, but fragments of files left by the constant write and overwrite of information caused by the deletion of existing files and the creation of new files. For example, a portion of an old file may be left behind when a new file is overwritten in the same space so called file slack space. The space between the end of a file and the end of the disk cluster it is stored in. Also called "file slack," it occurs naturally because data rarely fill fixed storage locations exactly, and residual data occur when a smaller file is written into the same cluster as a previous larger file. In computer forensics, slack space is examined because it may contain meaningful data [3].

The extraction of the data from the drive is based on the file system(s) present on the drive and may include data from such areas as active files, deleted files, file slack, and unallocated file space. Steps to extract these may include:

- Extraction of the file system information to reveal characteristics such as directory structure, file attributes, file names, date and time stamps, file size, and file location;
- Data reduction to identify and eliminate known files through the comparison of calculated hash values to authenticated hash values;
- Extraction of files pertinent to the examination. Methods to accomplish this may be based on the file name and extension, file header, file content, and location on the drive;
- Recovery of deleted files;
- Extraction of password-protected, encrypted, and compressed data;
- Extraction of file slack; and
- Extraction of the unallocated space.

If the alleged criminal left evidence of the crime in a computer, perhaps in e-mail or Word document, then finding evidence might not be so difficult. But criminal investigators often turn up computers whose owners took steps to destroy incriminating evidence. And that is when things get more difficult. One case has been documented involving a CEO whose bank had just merged with another. There was room for just one CEO, which was a problem for this soon to be redundant chief executive. An hour before the board meeting he accessed, modified and tried to destroy about 300 files without the proper tools. Properly deleting something not only requires the right tools but knowledge about everywhere that information is stored. Most people are not aware of temporary files. When a Microsoft Word document is created, there can be 14 temporary files created and therefore 14 slack dumps are created. After analyzing the file system, directory structure, file header and unallocated space, the CEO was prosecuted. Investigators, during their research, noted this false assumption about "deleting" a file, which ironically aids computer forensics examiners [2]. The pattern of file deletions and associated metadata can further compound the weight of evidence against the accused. Based on their experimentation they came up with their definition of file slack as data stored in non-traditional computer storage areas and formats.

Understanding data is a prerequisite to computer forensics investigations. For instance, just booting up a computer and opening files can fill the swap file with new data, perpetually edging out partial copies of files that may provide valuable evidence. Investigators came up with the notion that it is important to first collect and freeze the evidence before analyzing it. Data can be concealed on a computer system. Data hiding analysis can be useful in detecting and recovering such data and may indicate knowledge, ownership, or intent. Digital data hiding is actually a cluster-concept that spans many contexts. In modern times, non-physical data hiding is usually associated with digital forms such as cryptography, steganography, and watermarking [10]. NTFS file systems also offer some unique opportunities for data hiding. The NTFS file systems used today contain innovations that provide efficient file access (for instance, B-Tree organization of files within directories) and readily accessible metadata files to manage disk organization (Microsoft's version of resource forks called Alternate Data Streams), and some other small file storage oddities as well. When seeking to hide data, there are various strategies that might be employed. In general sense, metadata manipulation may be used to conceal covert data in bad clusters (\$BadClus). In fact, this same concept can be extended easily on an NTFS file system by working directly with the \$Bitmap file. The \$Bitmap file contains a complete map marking the allocation status of every addressable cluster in the partition. Should a consistency check be run, it would become obvious should someone modify this table

to hide data, but otherwise this provides a avenue for hiding data in a way that allows that data to persist for the life of the file system [5].

Methods of detection that can be used include:

- Matching the file headers to the corresponding file extensions to identify any mismatches. Presence of mismatches may indicate that the user intentionally hid data;
- Gaining access to all password-protected, encrypted and compressed files, which may indicate an attempt to conceal the data from unauthorized users. A password itself may be as relevant as the contents of the file;
- Steganography; and
- Gaining access to a host-protected area (HPA). The presence of user-created data in an HPA may indicate an attempt to conceal data [1].

H. Registry Investigation

The Windows registry contains a great deal of information, which may have evidential value or be helpful in aiding forensic examiners in other aspects of forensic analysis. Windows Vista stores configuration data in the registry. It is a central repository for configuration data that is stored in a hierarchical manner. System, users, applications and hardware in Windows make use of the registry to store their configuration and it is constantly accessed for reference during their operation. The registry is introduced to replace most text-based configuration files used in Windows 3.x and MS-DOS, such as .ini files, autoexec.bat and config.sys. Due to the vast amount of information stored in the Windows registry, the registry can be an excellent source for potential evidence. For instance, the Windows registry contains information on user accounts, typed URLs, network shared, and Run command history.

There are 5 root keys (i.e. starting point) in Windows registry. Table 2 shows the root keys and the abbreviation normally used.

Each key has one or more values. There are 3 parts in value, which are Name, Type and Data, as shown in Table 3.

When a software application reads values data in REG_BINARY from the registry, the application decides on how to decode the value. Applications can store data in binary (using REG_BINARY type) using their own data structure, hence only the application knows how to interpret it. For instance, interpreting REG_BINARY data as 8-bit ASCII or 16-bit Unicode could result in two different values. This technique could be used to hide data or at least confuse forensic examiner. Alternatively, some applications store REG_SZ and REG_DWORD data in REG_BINARY value, decoding and finding them can be difficult.

Criminals can use this technique to hide data. Programs can use four-byte REG_BINARY and REG_DWORD values (32-bit) interchangeably. Since an Intel x86-based system uses little endian architecture, REG_BINARY 0x01 0x02 0x03 0x04 is equivalent to REG_DWORD 0x04030201. Regardless of values type, the registry actually stores all values in binary format in the actual file. Since all values are stored alongside with their corresponding type, it allows the Registry Editor to interpret the values data correctly [13].

The Registry Editor only shows the logical structure of the registry. Physically, the registry is not stored on a single file in the hard drive [11]. Windows stores the registry in a few separated binary files called “hives”. For each hives file, Windows creates additional supporting files that contain backup copy of the respective hives to restore the hives during failed system boot. Only HKLM and HKU has corresponding hives (since the rest are symbolic links). However, none of 5 root keys are directly linked to a hives file. A suspect could hide all sorts of data, including a password, text information and binary files in the registry. A suspect could effectively hide data as registry key value entries. By using different encoding techniques, a suspect could obfuscate data from forensic examiner. Furthermore, the Register Editor has an implementation flaw that could potentially allow a suspect to hide data [7].

Several new registry files have been added to Windows Vista. The following list represents all the registry hives on a default Vista system which an investigator can analyze:

```
C:\Boot\BCD
C:\Windows\System32\config\RegBack\SECURITY
C:\Windows\System32\config\RegBack\SOFTWARE
C:\Windows\System32\config\RegBack\DEFAULT
C:\Windows\System32\config\RegBack\SAM
C:\Windows\System32\config\RegBack\COMPONENTS
C:\Windows\System32\config\RegBack\SYSTEM
C:\Windows\System32\config\BCD-Template
C:\Windows\System32\config\COMPONENTS
C:\Windows\System32\config\DEFAULT
C:\Windows\System32\config\SAM
C:\Windows\System32\config\SECURITY
C:\Windows\System32\config\SOFTWARE
C:\Windows\System32\config\SYSTEM
C:\Windows\winsxs\x86_microsoft-windows-b...-
bcdtemplate
client_31bf3856ad364e35_6.0.6000.16386_none_25ed
b26a062d63a9\BCD-Template
```

The user’s NTUSER.DAT file is still located in the root of the user’s root folder (C:\Users\). Note that Windows Vista now uses the “REGBACK” folder instead of the “REPAIR” folder that earlier versions of Windows use for backup copies of the registry.

The contents of the recycle bin has changed in Windows Vista and the name of the folder itself has changed

to "\$Recycle.bin". The INFO2 file that is present in earlier versions of Windows has been removed. In Windows Vista, two files are created when a file is deleted and placed into the recycle bin. Both files have the same random looking name, but the names are preceded with a "\$R" or "\$I". The file with the "\$R" at the beginning of the name is actually the data of the deleted file. The file with the "\$I" at the beginning of the name contains the path of where the file originally resided, as well as the date and time it was deleted. This is especially important for forensics examiners, particularly if the accused has tried to conceal or destroy evidence.

All registry keys have a value called "LastWrite" time, which is similar to file's last modification time. In fact, this value is a FILETIME structure, which is the same as file's MAC (Modified, Accessed, Created) time. The FILETIME structure is a 64-bit value representing the number of 100-nanosecond intervals since January 1, 1601 UTC [8], this was a feature added to Vista. However, an investigator could only obtain the registry key LastWrite time, but not the registry value LastWrite time. The LastWrite time will be updated whenever a registry value in the key is created, modified or deleted. Tools such as Keytime.exe, allows examiners to retrieve the LastWrite time of a specific key. Knowing the time of a key is modified or created allows forensic investigator to infer the approximate time an event or activity occurred. For instance, if a suspicious registry value is found in the registry's Run key, the investigator could query the LastWrite time of the key and compare it to the MAC time of the file to which the registry value is pointing. If there is a match between the key LastWrite time and the MAC time of the file to which the registry value is pointing, then the investigator will know the time that the registry value was created [12].

Since registry values support the binary data type, a suspect can store segments of program or the entire binary in the registry. These segments of program can be placed in several dispersed keys. Unless a forensic examiner knows the relevant keywords to search in the registry, then finding hidden data in tens of thousands of registry keys can be a tedious task.

An example of a place to hide data is in the time zone information key, HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\TimeZoneInformation. The hidden data can be the XML code, password, bank account number or some firm's business policies. This key contains time zone information, including the difference in minutes between UTC and the local time, as well as reference information during daylight saving time. Windows reads this registry key into TIME_ZONE_INFORMATION structure during system startup.

There are two strings in TIME_ZONE_INFORMATION structure, StandardName and DaylightName, of which can legally be an empty string. Any information written to them using the SetTimeZoneInformation() function is returned unchanged by the GetTimeZoneInformation() function).

Since Windows does not utilize these registry values, which are nested somewhere in some registry keys, and they are merely used for storing string information, a suspect can hide information such as passwords or passphrases in these values effectively. A suspect can modify the registry values for StandardName and DaylightName manually using Registry Editor to store information. Moreover, the suspect could retrieve this information using a piece of benign code by calling GetTimeZoneInformation() function which is loaded in Windows kernel32.dll without raising much suspicion, which came as an add-on feature in Vista.

III. USING HELIX IN A VISTA ENVIRONMENT

Helix is an open-source program based on Linux and is probably used by many forensic investigators to acquire volatile data. The Helix CD provides the OS and tools to audit and copy data from a suspect machine. The bootable Helix tool provides a graphical menu for accessing forensics tools. The tools, on the CD, allow for bit-for-bit copies of data to other media, providing the ability to recover deleted files, detect viruses (a hacker's system may be booby-trapped to destroy evidence), search out rootkits (used to hide hacker tracks) and look for hidden data. New obstacles have arisen as a result of Vista's new BitLocker AES-encrypted drive volumes. Forensics experts subsequently came up with a solution capture memory states for assessment. Disk encryption creates the need for new tools that can capture memory states in order to recover executable strings unpacked into RAM and copy them for later analysis.

The authors of this paper conducted an experiment, using Vista for live acquisition where a computer was shut down in an orderly fashion, through the use of commands as well as another instance where the computer electrical supply was pulled. These are the two scenarios with their implications for analysis:

- Orderly Shutdown Process
 - Possible loss of virtual memory space on disk.
 - Inability to control evidence destructive processes launched during shutdown.
- Pull the Plug
 - Loss of physical memory contents
 - Possible damage to open files and the file system

In both of the above cases, types of information located in memory which is subject to loss:

- Cached passwords (encryption, email, etc.)
- Memory resident only Malware code
- Fragments of open files, processes
- Shimmied kernel processes from backdoors
- Unencrypted data from encrypted disk source including PGP Whole Disk Encryption, SafeBoot.

IV. CONCLUSION

Windows Vista provides greater challenges to computer forensics investigators, especially as it pertains to encryption. Therefore, live acquisition becomes an even greater critical success factor for evidence collection. Future research in the field will necessitate investigators developing ways to break into an encrypted system or its files. Other features, such as scheduled defragmentation, are a serious challenge. The elimination of some evidence can also be seen in Microsoft's reduction in file metadata.

However, there are benefits to the forensics investigator. Scheduled file backups will indeed be helpful. With new changes in User Access Control, it will arguably be easier for a prosecutor to demonstrate ownership, control and intent, which are key tenets in the successful conviction of a perpetrator. There is still much research to be carried out on Vista but this paper has outlined the major ways in which the computer forensics investigator can effect a successful investigation.

ACKNOWLEDGMENT

The authors wish to acknowledge their friends in law enforcement who helped to make sure that the researchers are kept up to date with the latest security threats and thereby ensure that they are better instructors. Sincere thanks goes to Richard Britton, of the Manhattan's District Attorney's Office, who has provided invaluable advice.

REFERENCES

- [1] Andreas, S. "A parser to transform vista event log files into plain text". http://computer.forensikblog.de/en/2007/08/evt_parser.html August 2007.
- [2] Baryamureeba, V. "The Enhanced Digital Investigation Process Model" http://www.dfrws.org/2004/day1/tushabe_EIDIP.pdf, Nov. 2007.
- [3] Carvey, H. "Windows Forensics and Incident Recovery". Addison-Wesley, 2006.
- [4] Technet "Disabling last access time in windows vista to improve ntfs performance". blogs.technet.com/filecab/archive/2006/11/07/2006.
- [5] Garfinkel, S. "AFF: A New Format for Storing Hard Drive Images" . (Febraury 2006).
- [6] John, M. "Finding the user setting in vista". <http://www.devsource.com/article2/0,1895,19996337,00.asp>, Feb. 2006.
- [7] Microsoft. "Description of the Microsoft Windows Registry". <http://support.microsoft.com/default.aspx?scid=kb;EN-US;256986> (Sept. 2007)
- [8] Microsoft. *MSDN*. <http://msdn2.microsoft.com/enus/library/ms715237.aspx> (Jan 2008)
- [9] Microsoft. "Windows Live Mail." <http://morethanmail.spaces.live.com> (Nov. 2007)
- [10] Burghel, H. Hiding Data, Forensics and Anti-Forensics. 2007.
- [11] Carrier, B. *File System Forensic analysis*. Upper Saddle River, NJ 07458: Addison-Wesley. 2005.
- [12] SWGDE Technical Notes on Windows Vista. "Scientific Working Group on Digital Evidence(SWGDE)", Feb. 2008.
- [13] *File Extensions*. <http://www.filetext.com/harmful.htm> (Sept. 2005)

Value Parts	Description
Name	Every value has a unique name in that particular key.
Type	Values type determines the type of data value contains. The common value types in registry for instance are: REG_BINARY type contains binary data; REG_DWORD type contains double-word (32-bit) data; REG_SZ type contains fix-length string data.
Data	Values data contains data which usually relates to the values type.

Table I: Vista features by version

Vista Version	Home Premium	Business	Enterprise	Ultimate
BitLocker Drive Encryption			√	√
Encrypting File System		√	√	√
Shadow Copy		√	√	√
Complete PC Backup and Restore		√	√	√
Scheduled and Network Backup	√	√	√	√

Table II: Root Keys

Name	Abbreviation
HKEY_CLASSES_ROOT	HKCR
HKEY_CURRENT_USER	HKCU
HKEY_LOCAL_MACHINE	HKLM
HKEY_USERS	HKU
HKEY_CURRENT_CONFIG	HKCC

Table III: Value Parts

