

Potential Impacts of Windows Vista on Digital Investigations

Christopher Hargreaves and Howard Chivers

Abstract—Several of the new features of Windows Vista may create challenges for digital investigators. However, some also provide opportunities and create interesting new evidential artefacts which can be recovered and analysed. This paper examines several of these new features and describes methods for recovering volume shadow copies of files, identifying BitLocker on a system, the importance of recovery keys in dealing with BitLocker encrypted evidence and also describes the problems that User Account Control could cause for live investigations.

Index Terms— Computer Forensics, BitLocker, Live Analysis, Windows Vista,

I. INTRODUCTION

Windows Vista is the latest operating system from Microsoft and was released to the general public on 30th January 2007. It claims to be “the most secure version of Windows yet” [1], which, if true, is obviously beneficial for users of the operating system. However, several of its features may cause problems for other sections of the IT community including developers [2], and unfortunately forensic investigators.

This paper describes some of the challenges and also benefits to the forensic community that may result from the release and adoption of Windows Vista. It attempts to reduce the confusion and speculation that is prevalent in many forensic forums and websites and describes objectively how these new technologies may affect the quantity of available digital evidence.

The paper collects together and validates information and techniques used for obtaining evidence, many of which are scattered on the Internet, and also extends these techniques to contribute to existing knowledge regarding Windows Vista and forensics. It is intended that this paper provides a starting point for practitioners through a discussion of some relevant features and also some differences between old and new operating systems. It is hoped this will save practitioners time and resources during future investigations.

Paper received 30th April, 2007. C.J.Hargreaves, Cranfield University, Defence Academy of the United Kingdom, Shrivenham, SN6 8SW (+44 (0)1793 785753; e-mail: c.j.hargreaves@cranfield.ac.uk).

H.Chivers, Cranfield University, Defence Academy of the United Kingdom, Shrivenham, SN6 8SW (+44(0)1793 785656; e-mail: h.chivers@cranfield.ac.uk).

From Proceedings of Advances in Computer Security and Forensics (ACSF) 2007, Liverpool John Moores University

Academic literature is particularly devoid of information regarding Windows Vista and forensics, and it is hoped that this paper will expand this as a research area and highlight for the research community those areas that require further work.

This paper also contributes some practical work, in the form of a prototype tool for identifying previous versions of files, an examination of the different upgrade mechanisms of Vista and also validation of a technique to boot an imaged copy of Vista as a virtual machine.

It also highlights features of Vista which may cause problems for investigators that cannot be addressed by the development of new tools and therefore may require enhancements to the evidence collection methodology. This paper exists as part of a larger research project into identifying and balancing the risk of live investigations, and particularly while discussing the problem of full disk encryption presents evidence in support of a more flexible approach to evidence seizure.

This paper is not an exhaustive look into all the nuances of Windows Vista, which will manifest themselves as practitioners begin to encounter cases involving this new operating system. It also does not discuss Vista as an investigative platform, since compatibility and issues with specific forensic packages is likely to change rapidly.

The paper is organised as follows: Section II lists different editions of Microsoft’s new operating system and Section III comments on existing work on Vista and forensics. Section IV describes the overall methodology that was used during this research while investigating these new features. Section V discusses the mechanisms by which Vista can be installed and how this affects the amount of residual evidence recoverable from previous operating systems. Sections VI-XI then describe the individual features of Vista which may be of interest to the forensic community. The particular features discussed in this paper include reparse points, Volume Shadow Copies, BitLocker Full Volume Encryption, User Account Control and Vista’s backup features. The final sections summarise the limitations of this research, describe the advantages and disadvantages presented by Vista, offer conclusions and discuss future work.

II. WINDOWS VISTA EDITIONS

Windows Vista has five major versions and also slight variations for sale in the European Union and one for developing countries. The main versions are:

- Windows Vista Home Basic,
- Windows Vista Home Premium,
- Windows Vista Business,
- Windows Vista Enterprise,
- Windows Vista Ultimate.

Reference [1] offers a full and detailed comparison of features available in different editions of Windows Vista and will not be discussed in detail here. However, points of interest will be highlighted throughout the paper where it is relevant to the likelihood of encountering a particular feature.

III. PREVIOUS WORK ON VISTA AND FORENSICS

As mentioned in the introduction, there is limited information available regarding Vista and Forensics, particularly in academia. The most significant works on Vista and forensics are [3] and [4] which consist of a “high level look at what we know now about those changes in Vista which seem likely to have most impact on computer forensic investigators” [3]. The changes highlighted include descriptions of “built-in encryption, backup and system protection features”. These are also discussed in this paper but in greater detail and with additional contributions. Reference [4] also mentions the changing of Outlook Express to Windows Mail, the replacing of .evt files with an XML compliant format and changes to thumbs.db files. Since no additional contributions are made to these subjects in this paper, a discussion of them will not be repeated; although they remain areas requiring future work.

IV. METHODOLOGY

Features of Vista were selected based on their relevance to forensic investigations and the likelihood of making additional contributions to their understanding. For each feature that was examined, publicly available information from Microsoft provided an overview of the feature’s properties. Discussions in forensic forums and websites were also observed and provided background knowledge, and in some cases, the techniques proposed or information regarding a feature became the subject of experimentation in order to validate the described method. In some cases background information did not provide sufficient information to form hypotheses and in these situations the operation of features was observed to gain information about the location and structure of relevant digital artefacts which could then be confirmed through additional experimentation.

V. UPGRADE MECHANISMS

This section discusses mechanisms by which Vista may be installed on a system. This is particularly relevant if an upgrade has taken place so that evidence from earlier operating systems can be recovered. Four situations have been identified that describe the means by which Vista comes to reside on a system, and each leaves a different amount of residual digital evidence from the previous operating system. In each scenario Vista was installed and the disk examined to

determine the location, if any, of user data from the previous operating system.

1) *A clean install on a newly purchased system (possibly by the manufacturer):* This will not contain any relevant evidence prior to the date of the Vista installation unless it has been manually copied from an older system.

2) *Fresh install on an existing system, including formatting the drive:* In this instance, the system was booted from the Windows Vista DVD and the hard drive formatted as part of the installation process. After the installation the disk was examined and it was found that even after formatting, although the Master File Table (MFT) was replaced, the contents of some non-resident residual user files were still accessible in unallocated space. Unfortunately, it is not possible to quantify how much residual user data remains after a format since data in unallocated space is highly volatile and susceptible to being overwritten. This was demonstrated in experiments, since after continued use of the system the previously identified residual data was overwritten. However, the possibility of recovery does exist which reinforces the importance of research into file carving tools such as those developed for the 2006 DFRWS Challenge in order to recover data from this area of the file system.

3) *Fresh install on an existing system, without formatting:* This installation was performed by inserting the DVD into an existing live XP system. Two options were presented, which were: to upgrade the current system to Vista, or to perform a fresh installation. In this case a fresh installation was selected and when completed, the disk was examined. It was found that a folder Windows.old was created and populated with files and folders from the previous operating system, including the folders: Documents and Settings, Program Files and Windows. User data from the previous operating system can therefore be found in `\Windows.old\Documents and Settings\[Users]\`.

4) *A conventional ‘upgrade’ of an old operating system:* During this upgrade, previous user data was found to be contained in the new Users folder which replaces the Documents and Settings folder of Windows XP. In addition, folders outside the Documents and Settings folder were also preserved.

VI. FOLDER LOCATIONS AND REPARSE POINTS

There are several minor file system changes in all versions of Windows Vista that should be noted. At the most basic level, some file and folder locations have changed, including, Documents and Settings, which has been replaced with Users[5]. The same work describes how the storage of user data has changed inside this folder and also the extensive use of junctions and reparse points inside these folders.

In addition to the default reparse points used by Vista, they can also be implemented manually by advanced users using the built in mklink command as described in [6].

During experiments to identify reparse points, the Junction tool, available from [7] was used to list them on a live Vista system. Forensic packages were also used to identify reparse points on imaged disks, as shown in Figure 1.

These tools gave slightly inconsistent results and as a result it is important to recognise that reparse points can also be identified manually in the MFT by the C0 00 00 00 attribute header [8]. An examination of reparse points in the MFT indicated that the attribute contains the location to which the reparse point redirects, as shown in Figure 2. These can be used as part of a manual examination and verification of correct tool operation.

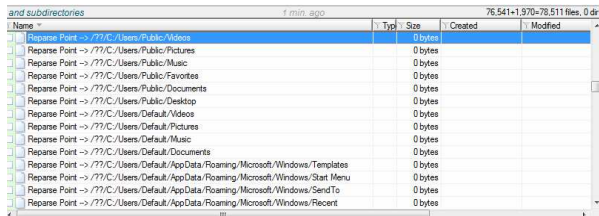


Fig. 1. X-Ways Forensics highlighting reparse points on a system

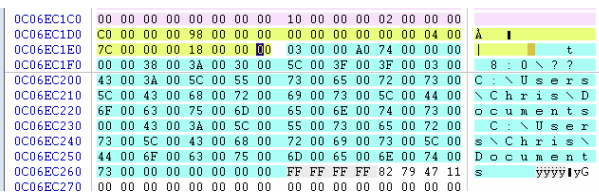


Fig. 2. An example reparse header extracted from the MFT. The attribute begins with C0 00 00 00.

VII. VOLUME SHADOW COPY

As will be discussed later, some of the new features of Vista may cause problems for future investigations. However, as pointed out in [3], “some of the new features can actually work to the forensic examiner’s advantage”. One such example is the intriguing Volume Shadow Copy feature. This extends the functionality of the System Restore Points created in Windows XP, so that user data is automatically backed up in addition to critical system files [9]. This feature is enabled by default and for users of Vista Business, Enterprise and Ultimate, it means that previous versions of stored files can be viewed, copied or restored [9] through the Vista user interface, as shown in Figure 3.

An analysis of XP system restore points is available in [10] and was used to examine system restore points in Vista. A test file set was created and as additional data was appended to these files and system restore points were created, it was found that unlike the description in [10], new sub-folders were not created for each restore point and there was no change.log which mapped backed up files to their originals. This indicated that the analysis technique in [10] does not extend to Vista, although the System Volume Information folder is still utilised.

The exact format of shadow versions is still not fully understood, but some preliminary experimental results are detailed here in the hope they will assist future research.

The shadow copies of files generated in experiments did not have entries in the MFT and were not stored with the originals. Instead they were stored within container files in the System Volume Information folder. Each system restore point created a new container file consisting of mini-file tables that contained shadow copies of the test files that were being modified in addition to system files. Both resident and non-resident data was contained within the system restore container files.

The Vista system restore container files were extracted using forensic software in an attempt to identify shadow copies of files. In the course of this research an experimental tool to parse extracted shadow copy container files was developed. This interpreted these mini-file tables as MFTs, examining each 1024 byte entry and extracting their attributes, particularly of interest are the Parent ID, which can be used to identify the file’s original location, and the size of the data attribute.

Future work will involve full validation of the results from this tool and also extracting these shadow file copies from the restore files and recovering them as evidential artefacts. However, an immediate methodology to preview shadow copies was also developed. This first involves using the tool above as an indicator of the existence of shadow copies. This was then followed by the use of VMware to boot an image file of the seized system as described in [11] and [12]. It was then possible to natively view shadow copies of files inside a virtualised version of the imaged copy of Windows Vista. This sidesteps any difficulty in manually reconstructing data from the restore point files.

However, it still remains important to verify the results from any tool with a second independent tool, or manually from the original data [13]. This is particularly true in this case since a virtualised but potentially untrustworthy operating system is used to recover evidence. Shadow copies are potentially lucrative areas for evidential artefacts and further research into their exact nature would be highly beneficial.

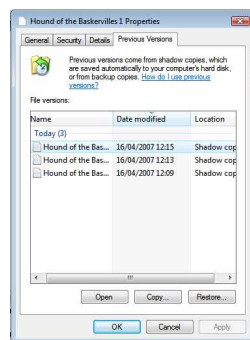


Fig. 3. Screenshot showing the previous versions of a file viewed through the Vista GUI

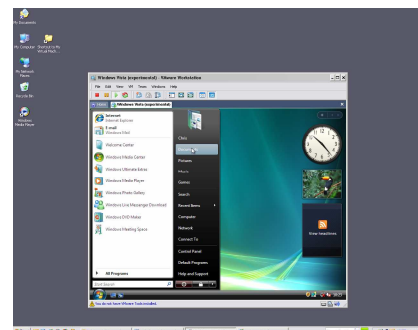


Fig. 4. Screenshot of an imaged Vista system being booted in VMware. It should be noted that LiveView [14] was used to convert acquired disk images into VMware disk files rather than mounting disk images as drive letters as described in [12] and [13].

VIII. DATE AND TIME STAMPS

The importance of dates and times in an investigation is well understood and is discussed in detail in [15], including a case study highlighting some of the pitfalls. It is therefore important to highlight that the automatic updating of the ‘last accessed’ aspect of the often used Modified Accessed Created (MAC) times is not enabled by default in Windows Vista for performance reasons [16]. However, it is possible for a user to manually enable these updates and to assist in detecting this, the registry key to determine the status of this functionality is given below, which is provided in [16] and was tested by modifying the value in the registry and verifying that ‘last accessed’ times were then updated.

```
HKEY_LOCAL_MACHINE\SYSTEM\Current Control
Set\Control\File System\NtfsDisableLastAccessUpdate\
```

IX. BITLOCKER FULL VOLUME ENCRYPTION

A. Introduction and discussion

According to [17], BitLocker is “a data protection feature available in Windows Vista Enterprise and Ultimate...[which] prevents a thief who boots another operating system or runs a software hacking tool from breaking Windows Vista file and system protections or *performing offline viewing of the files stored on the protected device.*” The functionality described in the last part of this definition has caused BitLocker to become one of the most hyped and speculated about features of Windows Vista, particularly in the forensic community. Rumours have included reports on talks between governments and Microsoft to discuss the implementation of backdoors [18], which have been strongly denied by those at Microsoft [19]. This speculation regarding backdoors will not be discussed further here and will be assumed to be untrue.

A more useful topic for discussion is whether BitLocker represents a significant challenge to digital investigations. Technically BitLocker could present difficulties compared with other types of encryption typically encountered on a system. This is because many of the approaches used to recover encrypted information rely not on breaking encrypted files themselves, but are based on the premise that data cannot be processed while it is encrypted, so must exist in a plaintext form to be manipulated in any way [20].

These techniques can involve recovering parts of the plaintext version of a now encrypted file, which may be possible if file deletion rather than file wiping was used [21]. Also it is possible for an encrypted file to be written to disk during memory swapping operations or stored temporarily while being processed [22]. The possibility also exists of locating passwords or keys on the disk which have once been in RAM and were at some point swapped to disk [23].

BitLocker and other full volume encryption software reduce the effectiveness of many of these approaches since the entire volume is encrypted [17], including locations such as unallocated space, the pagefile, and temporary folders where temporary decrypted data, keys or passwords may reside.

Reference [24] discusses if BitLocker represents a serious threat to forensics and contains a list of ‘mitigating factors’ and “their potential to reduce the impact of bit locker [sic] on the ability of digital forensic practitioners to read information from hard drives.” It should be made clear that the arguments presented in [24] suggest only that BitLocker may not be frequently encountered, rather than describing that means exist to minimise the impact that BitLocker has on an individual investigation. The ‘mitigating factors’ presented in [24] that describe why “the problem may not be as significant as first thought” are discussed below.

Availability and Cost: “Of the five different versions of Windows Vista that will be available upon its release, only two of them contain the bit locker technology. Additionally, the two versions that will contain this technology are also the most expensive” [24]. Whilst this is true and in the UK Vista Ultimate does cost in excess of £300 [25]; it is possible for home users to obtain an OEM copy for just £122. While this may be a violation of the End User Licensing Agreement it does not mean it will not occur [26] and as a result, cost is much less of a deterrent than [24] describes.

Hardware Requirements: The need for a Trusted Platform Module (TPM) chip is described as “probably the most significant barrier to the use or adoption of bit locker [sic]” [24]. This is based on a survey of PCs for sale by IBM, HP and Dell in Australia. The study concluded that TPMs were found predominantly in systems designed for business use, rather than home users and were not widely available. A study in the UK is yet to be carried out; however, if one required or desired a system containing a TPM chip, a budget laptop containing the technology to run BitLocker is available for less than £400 [27]. Furthermore, it is possible to run BitLocker without the use of a TPM by storing keys on a USB memory stick [17], which are readily and cheaply available.

Off by Default: Here [24] states that many encryption technologies already exist and are simply not utilised by offenders. Whilst file/disk encryption may not be in common usage, the Home Office in the UK reports that the use of encryption is increasing and as a result “investigators have begun encountering encrypted and protected data with increasing frequency” [28]. This does not necessarily mean that BitLocker will become the encryption product of choice but it is one that will be available to those who choose to encrypt their data.

Adoption Rate: Reference [24] describes that similarly to the case with the Windows ME to XP upgrade, it takes some time before new operating systems are encountered frequently for examination and there are fewer incentives to upgrade from XP to Vista. However, with Windows XP no longer being supplied on new PCs from large manufacturers such as Dell, HP and Toshiba from 31 January 2008 [29], the sentiment from [3] that “this new OS will continue the trend of Microsoft’s dominance in the operating system market and wise computer forensics professionals will want to start thinking about the implications now” seems a sensible

approach for the research community to adopt and supports the pre-emptive ethos of this paper.

Only Allows Encryption of OS Volume: Reference [24] also reports that BitLocker is only capable of encrypting a single volume, the Operating System volume. Reference [30] describes how to encrypt other data volumes using command line scripting and in any case it also allows either the Encrypting File System (EFS) or a third party encryption package to protect other drives and BitLocker to then protect any data or keys leaked to the operating system volume [31].

In summary, some of the sentiments in [24] are valid; particularly that it is turned off by default and the limited availability of BitLocker in the range of Vista versions available. It does therefore seem that BitLocker is unlikely to interfere with the majority of investigations. However, these ‘mitigating factors’ may not be as significant as described and as mentioned earlier, encryption is currently in use and that use is increasing. There are also no obstacles to obtaining the hardware and software needed to run BitLocker which cannot be easily overcome.

It is the intention of this paper to discuss BitLocker before it is encountered in investigations, not after, and to this end the following sections describe methods for the detection of BitLocker and what is necessary during the seizure stage to ensure that later access to evidence on BitLocker volumes is possible.

It should be noted that many of the methods discussed involve performing actions on a live system. The risks of live investigations are part of an ongoing research project and will be discussed in detail in a future paper. However, [32], [33], [34] and [35] provide insight into some of the difficulties and as always ACPO Principle 2 “In exceptional circumstances, where a person finds it necessary to access original data held on a computer or on storage media, that person must be competent to do so and be able to give evidence explaining the relevance and the implications of their actions” [36], strongly applies.

B. BitLocker Operation

A detailed description of BitLocker’s operation including the utilisation of TPMs is included in [17] and will not be reiterated here.

For investigators it is useful to know the different modes in which BitLocker can operate. These are:

TPM only: This is the simplest scenario and the encryption keys are protected by the TPM. The system will boot with no user intervention, but the disk will not be able to be moved to a new platform [17] for imaging.

TPM + PIN: Keys are protected by the TPM and a PIN must also be entered with the function keys for every boot or resuming hibernation [17].

TPM + USB: Keys are protected by the TPM and a USB storage device containing a start up key must also be provided for each boot [17].

USB only: This can be used if a TPM is not enabled or not

present. Start up keys are stored on a USB stick and must be provided in order for the system to boot. In this case the keys take the form of a 124 byte, hidden, read-only file, which by default has a file name of the format XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXXXXXXX.BEK, where X is a hexadecimal digit [37].

At time of writing, during experiments performed as part of this research, only the ‘USB Only’ BitLocker mode has been examined.

C. Identification of BitLocker

BitLocker is only available in Enterprise and Ultimate editions of Vista [1] so identification of other versions of Vista can rule out the presence of BitLocker. This can be achieved on a live system using the psinfo tool [38] or by examining the system properties through the control panel.

If an appropriate version of Vista is installed, due to the requirement for a 1.5 Gigabyte system partition which must remain unencrypted [17], the drive partitioning may be the first sign to indicate the presence of BitLocker.

Reference [39] describes the development of a script to report if BitLocker is operating. This has not been tested as part of this research since [30] describes the use of built-in scripts to show the status each volume. These were tested and sample output is shown in Figure 5. Running untrusted scripts on a suspect system is unwise but the technique could be more acceptable if these scripts were copied in advance to form part of a trusted forensic CD and were executed only from this read only medium [32].

```

Administrator: C:\Windows\System32\cmd.exe
C:\Windows\system32>script manage-bde.wfs -status
Microsoft (R) Windows Script Host Version 5.7
Copyright (C) Microsoft Corporation. All rights reserved.

Disk volumes that can be protected with
BitLocker Drive Encryption:
Volume C: [
[OS Volume]

Size: 48.04 GB
Conversion Status: Fully Encrypted
Percentage Encrypted: 100%
Encryption Method: AES 128 with Diffuser
Protection Status: Protection On
Lock Status: Unlocked
Key Protectors:
    External Key
    Numerical Password

C:\Windows\system32>
  
```

Fig. 5. Results of running the built-in manage-bde.wfs script identifying encrypted volumes on a live system

A Microsoft Developer Network (MSDN) article [40] describes an alternative method for detecting BitLocker if scripts cannot be run, i.e. if the machine is powered off, and relies on inspecting the boot sector. An examination of sector 0 of each partition was performed, and a hex-dump of the boot sector of the operating system partition of a machine running BitLocker is shown in Figure 6. There are several methods described here and correlating results from different methods, particularly on a live system increases the chances of obtaining accurate results [34].

Offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	
00000000	EB	52	90	2D	46	56	45	2D	46	50	2D	00	02	08	00	00	eRI-FVE-FE-
00000016	00	00	00	00	F8	00	00	3F	00	FF	00	00	E8	2E	00		ø ? ý è.
00000032	00	00	00	80	00	80	00	FF	3F	01	05	00	00	00	00		! ! ý?
00000048	00	00	04	00	00	00	00	6E	2D	02	00	00	00	00	00		n-
00000064	F6	00	00	01	00	00	00	D5	54	12	AC	72	12	AC	8E		ó ÔT -r -I
00000080	00	00	00	FA	33	C0	8E	D0	BC	00	7C	EB	68	C0	07		ú3AIBW ahA
00000096	1F	1E	68	66	00	CB	88	16	0E	00	66	81	3E	03	00		hf Et fI> H

Fig. 6. Hex dump of a boot sector from a Vista operating system volume indicating the presence of BitLocker

D. Recovering Data from BitLocker Enabled Systems

If a system is discovered in a powered off state and is using BitLocker it is unclear how successful an investigation will be and a discussion of possible vulnerabilities of the specific Microsoft full volume encryption implementation and hardware attacks on TPMs are outside the scope of this paper. However, results from experiments performed as part of this research show that obtaining recovery keys can greatly assist in extracting evidence from an encrypted volume. The use of recovery keys is described in the next section.

Recovery keys are created in addition to the encryption keys generated when the BitLocker is activated. Their purpose is to allow access to encrypted data if the encryption keys are lost, the PIN is forgotten, an encrypted volume is moved to a new system and other scenarios, see [17]). During the BitLocker life cycle, keys are created prior to encrypting the drive and can be stored on USB drives, any other accessible folder or printed [17]. During all experiments, recovery keys were found to be stored by default with a .TXT extension with filename of the format XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX.TXT, where X is a hexadecimal digit.

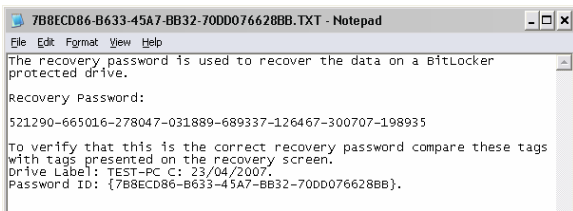


Fig. 7: Shows typical contents of a recovery key file

In terms of recovering evidence from a system, if it is encountered in a powered on state, experiments have shown it may be possible to obtain a live, complete disk image. This was achieved by creating a logical disk image using FTK Imager since accessing the physical disk copied data in its encrypted form, as shown below in Figure 8.

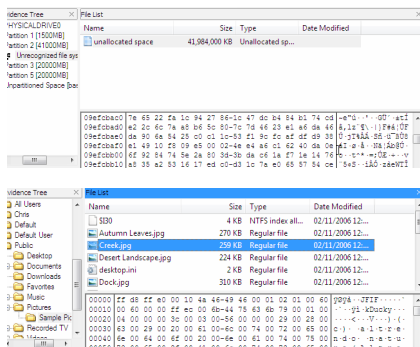


Fig. 8: Physical (top) vs. Logical (bottom) acquisition of a live system running BitLocker. Logical provides access to the file system on a partition but a physical image works below the full disk encryption driver and images the raw encrypted data.

In addition to obtaining disk images from a live system, it was also possible to create backup copies of the start-up or recovery keys by accessing the 'Manage BitLocker Keys' interface through the control panel, as shown in Figure 9. This

allowed later recovery of potential evidence from the disk as described in the following section.

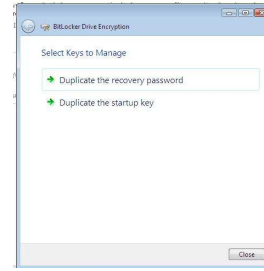


Fig. 9: Exporting BitLocker recovery keys from a live system

E. Evidence from a Seized Drive Using Recovery Keys

Using the recovery keys it was possible to boot a system protected by BitLocker in order to create a logical image and access the unencrypted data. Obviously this is not a desirable way to recover evidence since it unnecessarily accesses the original evidence. To resolve this problem, the physical drive was imaged offline and LiveView [14] was used to convert the disk image into a VMware virtual machine disk file. At this point it was possible to boot the virtual version of the original system using the recovery keys and obtain a logical image, which as described earlier provides unencrypted data.

However, this imaging relies again on a virtualised but untrusted operating system. To resolve this problem a second virtual machine was created, Vista Ultimate edition was installed and the converted image from the original machine was added to the new system as a second virtual drive. By booting into this freshly installed virtual Vista machine and using the BitLocker interface it was possible to unlock the drive using the recovery keys and produce a logical, unencrypted image of the original drive using a trusted operating system.

This has an advantage over connecting the original physical drive through a write blocker to a real Vista system to perform this drive unlocking and imaging since the initial disk imaging stage of the investigation remains the same. This disk image is then used for the entire analysis and recovery of evidence.

F. BitLocker Conclusions

In summary, BitLocker may not be encountered in every case and may not cause widespread problems for digital investigators. However, in cases where it is encountered it could provide a significant challenge.

Identification of BitLocker can be performed on a live system and if detected, imaging of logical volumes is possible, as is exporting the recovery key, which has been shown to be extremely useful in the retrieval of BitLocker encrypted data. Even if a system is not powered on, it may be advantageous to perform a quick analysis of the boot sector *in situ* using a forensically sound technique. If BitLocker is found to be present, the locating of recovery keys on USB devices, other digital media or on printouts may be vital to successfully gaining access to evidence and can be appropriately prioritised.

X. USER ACCOUNT CONTROL

The goal of User Account Control (UAC) is to allow users to run standard privilege accounts, only escalating privileges to administrator if necessary [41]. Standard user accounts exist in Windows XP (Limited account) but are restrictive and inconvenient and as a result “working with this type of account has been so difficult that many organisations choose to give users administrator privileges” [42].

Vista aims to change this, firstly by allowing many previously administrator-only operations to be performed by standard users, including time-zone changes, wireless network configuration, power management settings, adding printers, installing critical Windows updates [2]. Secondly, when an action is performed that requires administrator privileges, the user is informed of this and is then able to seamlessly escalate their privileges to administrator [42].

UAC has some implications for investigators since many of the live tools and techniques discussed earlier require administrator privileges. The two types of account that can be created in Vista are similar to XP: a standard user and an administrator account, although even the ‘administrator’ account runs processes with standard privileges [2]. During experiments, UAC did not pose a problem if the account was administrative since even though confirmation was required to run processes with real administrator privileges, it was as simple as clicking ‘allow’, as shown in Figure 10.

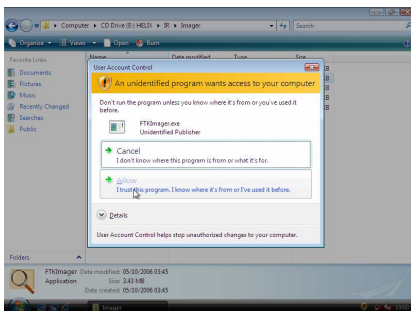


Fig. 10: Running a process with ‘real’ administrative privileges

The difficulty arose if an account was run as a standard user, which may be more likely due to the more integrated privilege escalation method. When administrative actions were performed in a standard account, a password was required, which an investigator running live tools on a suspect’s system may not have access to. This caused problems running tools correctly. For example, FTK imager was run without administrator privileges and could not create logical or physical image of a system and was restricted to logical file-level imaging only.

Therefore, one of the true challenges of Vista may be if BitLocker is used in conjunction with UAC. In this case the full volume encryption protects against an offline analysis and UAC severely limits the effectiveness of a live investigation to the current, non-system active file set. This excludes unallocated space, the registry, the pagefile and any other protected files from an investigation, many of which are a rich source of potential digital evidence.

This further emphasises the importance of obtaining the recovery keys of BitLocker volumes since UAC is not effective if the operating system is not running.

If recovery keys are known not to be available, the logistics of a seizure may become more important and timing a seizure so that not only is a machine live, but live and running an administrative account. Alternatively, surveillance may become necessary to obtain administrator passwords, although with the system protection features offered by Vista this may need to be hardware based rather than software. This is yet another subject requiring further research.

XI. BACKUP FEATURES OF WINDOWS VISTA

One consequence of the difficulties presented by BitLocker and UAC is the importance of recovering backup files. Vista backups can be made to an external drive, CD or DVD so it is important that such media are collected. Reference [43] discusses how to identify from the registry when and to where backups were made, and also which types of file were included in the backup [44]. If this information can be recovered on site (in a forensically sound manner) it may help focus the search for physical evidence upon which important backups may reside.

XII. LIMITATIONS

As mentioned in the introduction, this paper is not an exhaustive look at Windows Vista and forensics. There are many more features than those listed here which will be of interest to investigators and researchers. These may include: changes to the registry, new log files, superfetch, Windows Mail and Internet Explorer 7.

Those features which are discussed in this paper have had only a short introduction and some would warrant their own paper to discuss all the details. BitLocker in particular is an area of great interest and is part of ongoing research.

The experiments performed as part of this research were all performed on fresh installs of the 32-bit version of Vista in controlled environments, many on virtual machines. It is unknown how the installation of additional software, updates and service packs to Windows Vista will affect the results.

Finally, many of the techniques described here involve the use of live tools on a system which are discussed without mentioning the consequences of performing actions on a live machine. Live tool testing is part of ongoing research and will be the subject of a future paper.

XIII. CONCLUSIONS AND FUTURE WORK

This paper has compiled and validated much of the information available on Windows Vista and forensics and has also made some new contributions, particularly identifying shadow copies and the use of virtualisation to recover evidence from shadow copies and BitLocker.

The paper also supports a more flexible approach to evidence collection, and while not fully encouraging live analysis, highlights that further research into this area is needed and the option should not be totally excluded from an investigator’s mind since in some cases it may be the only

means to gain access to evidence. Also, *in situ*, forensically sound analyses of systems at the scene e.g. bootable CDs, could assist in identifying the locations of backup media or detecting BitLocker so that a search for recovery keys can be prioritised.

Windows Vista has been shown to provide both challenges in the form of BitLocker, but also opportunities, such as Shadow Copies of files. It has also, hopefully, highlighted for the research community how many opportunities for research are provided by Vista and how this will benefit the practitioner community. Since practitioner research is often case driven, and cases involving Vista may not appear for some time, academia can greatly assist by performing such pre-emptive research in this area of digital forensics.

REFERENCES

- [1] Microsoft (2006), 'Windows Vista Product Guide', <http://www.microsoft.com/downloads/details.aspx?FamilyID=bbc16ebf-4823-4a12-afe1-5b40b2ad3725&DisplayLang=en>
- [2] Moth, D. (2006), 'Windows Vista Security Features for Developers: User Account Control', MSDN Event (Reading), Slides available at: http://download.microsoft.com/documents/uk/msdn/events/Daniel_Moth_User_Account_Control.ppt
- [3] Morris, J. (2007), 'Notes on Vista Forensics, Part One', <http://www.securityfocus.com/print/infocus/1889>
- [4] Morris, J. (2007), 'Notes On Vista Forensics, Part Two', <http://www.securityfocus.com/infocus/1890>
- [5] Mueller, J. (2006), 'Finding the User Settings in Vista', <http://www.devsource.com/article2/0,1895,1999637,00.asp>
- [6] Russinovich, M. (2007), 'Inside the Windows Vista Kernel: Part 1', TechNet April, 14-19.
- [7] Russinovich, M. (2006), 'Junction v1.04', <http://www.microsoft.com/technet/sysinternals/FileAndDisk/Junction.msp>
- [8] Carrier, B. (2005), File System Forensic Analysis, Addison Wesley., p.282.
- [9] Microsoft (2007), 'Learn about the features: Shadow Copy', <http://www.microsoft.com/windows/products/windowsvista/features/details/shadowcopy.msp>
- [10] Harms, K. (2006), 'Forensic analysis of System Restore points in Microsoft Windows XP', Digital Investigation 3, 151-158.
- [11] Baca, E. (2002), 'Using Linux VMware and SMART to Create a Virtual Computer to Recreate a Suspect's Computer', http://www.infosecwriters.com/text_resources/andrewrosen/SMARTForForensics.pdf
- [12] Penhallurick, M. A. (2005), 'Methodologies for the use of VMware to boot cloned/mounted subject hard disk images', Digital Investigation 2, 209-222.
- [13] Carrier, B. (2003), 'Defining Digital Forensic Examination and Analysis Tools Using Abstraction Layers', International Journal of Digital Evidence 1(4).
- [14] Kaplan, B. (2007), 'Live View', <http://liveview.sourceforge.net/>.
- [15] Boyd, C. & Forster, P. (2004), 'Time and date issues in forensic computing - case study', Digital Investigation 1, 18-23.
- [16] Anon (2006), 'Disabling Last Access Time in Windows Vista to improve NTFS performance', <http://blogs.technet.com/filecab/archive/2006/11/07/disabling-last-access-time-in-windows-vista-to-improve-ntfs-performance.aspx>
- [17] Microsoft (2006b), 'BitLocker Drive Encryption: Technical Overview', <http://www.microsoft.com/technet/windowsvista/security/bittech.msp>
- [18] Stone-Lee, O. (2006), 'UK holds Microsoft security talks', http://news.bbc.co.uk/1/hi/uk_politics/4713018.stm
- [19] Ferguson, N. (2006), 'Back-door Nonsense', http://blogs.msdn.com/si_team/archive/2006/03/02/542590.aspx
- [20] Denning, D. E. (1999), Information Warfare and Security, Addison Wesley, p. 309.
- [21] Zimmermann, P. (1998), PGP User's Guide, PGP, chapter Appendix C: Phil Zimmermann on PGP, pp. 139-166.
- [22] Casey, E. (2002), 'Practical Approaches to Recovering Encrypted Digital Evidence', International Journal for Digital Evidence 1(3).
- [23] Craiger, J. P.; Pollitt, M. & Swauger, J. (2005), 'Law Enforcement and Digital Evidence', <http://ncfs.org/craiger.delf.revision.pdf>
- [24] Woodward, A. (2006), 'BitLocker - the end of digital forensics?', Proceedings of 4th Australian Digital Forensics Conference December, 18-28.
- [25] Amazon (2007), 'Windows Vista Ultimate Edition', <http://www.amazon.co.uk>
- [26] Honeyball (2007), 'Vista: an inquest', PC Pro 152, 160-162.
- [27] E-Buyer, 'HP NX6325', <http://www.ebuyer.com/UK/product/124974>
- [28] Home Office (2006), 'Investigation of Protected Electronic Information: A public consultation', <http://www.homeoffice.gov.uk/documents/cons-2006-ripa-part3/ripa-part3.pdf>
- [29] BBC (2007), 'Windows XP to be retired in 2008', <http://news.bbc.co.uk/1/hi/technology/6551429.stm>
- [30] Microsoft (2007a), 'How to encrypt data volumes in Windows Vista', <http://support.microsoft.com/kb/933637>
- [31] Microsoft (2007b), 'Will BitLocker encrypt more than just the operating system volume?', <http://technet2.microsoft.com/WindowsVista/en/library/58358421-a7f5-4c97-ab41-2bcc61a58a701033.msp?mfr=true>
- [32] Adelstein, F. (2006), 'Live Forensics: Diagnosing your system without killing it first', Communications of the ACM 49(2), 63-66
- [33] Carrier, B. (2006), 'Risks of Live Digital Forensic Analysis', Communications of the ACM 49(2), 56-61.
- [34] Carvey, H. (2004), 'Instant Messaging Investigations on a Live Windows XP System', Digital Investigation 1(4), 256-260.
- [35] Kenneally, E. E. & Brown, C. L. (2005), 'Risk Sensitive Digital Evidence Collection', Digital Investigation 2(2), 101-119.
- [36] ACPO (2003), Good Practice Guide for Computer Based Electronic Evidence, Association of Chief Police Officers.
- [37] Microsoft (2006c), 'BitLocker Drive Encryption: Value-Add Extensibility Options', <http://download.microsoft.com/download/a/f/7/af777e5-7dcd-4800-8a0a-b18336565f5b/BitLockerExt.doc>
- [38] Russinovich, M. (2006), 'PsInfo v1.74', <http://www.microsoft.com/technet/sysinternals/utilities/psinfo.msp>
- [39] HogFly (2007), 'Detecting BitLocker', <http://forensicir.blogspot.com/2007/03/detecting-bitlocker.html>
- [40] Hunter, J. (2006), 'Detecting BitLocker', http://blogs.msdn.com/si_team/archive/2006/10/26/detecting-bitlocker.aspx
- [41] Microsoft (2006d), 'User Account Control Overview', <http://technet.microsoft.com/en-us/windowsvista/aa906021.aspx>
- [42] Microsoft (2006e), 'How Windows Vista Helps Protect Computers From Malware', <http://technet.microsoft.com/en-us/windowsvista/aa940967.aspx>
- [43] HogFly (2007a), 'Vista Complete Backups: Part 1', <http://forensicir.blogspot.com/2007/03/vista-complete-system-backup.html>
- [44] HogFly (2007b), 'Vista Complete Backups: Part 2', <http://forensicir.blogspot.com/2007/03/vista-complete-backups-part-2.html>