

Microsoft Vista: Serious Challenges for Digital Investigations

Darren R. Hayes and Shareq Qureshi

Seidenberg School of CSIS, Pace University, New York
{dhayes@pace.edu, sq05639n@pace.edu}

ABSTRACT

Microsoft's Vista ("Vista") can be seen as a dramatic departure from previous versions of the vendor's operating systems, in terms of security and file systems. This vendor's technical advances in security have created problems for law enforcement and other computer forensics investigators. This paper will illustrate how changes to Vista's file systems will impede the retrieval of inculpatory evidence by prosecutors; the discovery of digital evidence on a system is more problematic in a Vista environment. The successful conviction of a defendant is reliant upon a prosecutor effectively demonstrating control, ownership and intent relating to the data found on the perpetrator's computer. However, a machine running Vista is likely to negatively impact these findings. This paper will seek to guide the forensics investigator through the plethora of Vista operating system changes and provide suggestions for alternative methods of data discovery.

Keywords

Vista, BitLocker, Encryption, Operating Systems, Computer Forensics

I. INTRODUCTION

The paper will detail the findings of scientific experiments, conducted in the Seidenberg School's Computer Forensics Laboratory. Through collaboration with the Manhattan District Attorney's Office, the computer forensics research group was able to research key files types that are of interest to prosecutors of criminal investigations. Subsequently, this research has provided information about the challenges expected to be encountered within a Vista environment and ultimately provide helpful recommendations to investigators. The research herein merely highlights some of the results, which pertain to files, especially in regards to defragmentation, restoration, metadata, event logs, indexing and storage.

A. Defragmentation and Restore

The defragmentation program on Vista is different to the one on previous versions of Windows as there is no longer a graphical display of the process. Most importantly, defragmentation in Vista is set to automatically run once a week. We know from Carrier that some defragmentation occurs periodically in previous versions of Windows unbeknownst to us. However, defragmentation is run automatically in

Vista (Carrier B. , 2005). A defragmentation can also be executed manually in Vista if necessary. Either way, it works in the background at a low priority without a graphical display. Defragmentation can also run from an administrative command prompt. To perform this, click on the start orb and type 'cmd' in the search box. Do not press enter. Instead, hold down 'Ctrl', 'Shift' and then press enter. After providing administrative credentials, you will be at the command prompt. If you do this correctly, the prompt will read 'C:\Windows\system32>'. At this prompt, type 'defrag /?' for a full list of the defragmentation commands together with a few examples. To get a detailed report of the fragmentation status, enter 'defrag C: -a -v'. To perform a full defragmentation, enter 'defrag C: -w' or 'defrag C: -w -f' to force a defragmentation if you have low disk space. Note that in both cases you can add the switches '-a' and '-v' if you want more detailed output. Why is this important? Its importance stems from the fact that with the advent of automatic defragmentation, computer forensics investigators will face a significant decrease in evidentiary data (Microsoft, Description of the Microsoft Windows Registry, 2007).

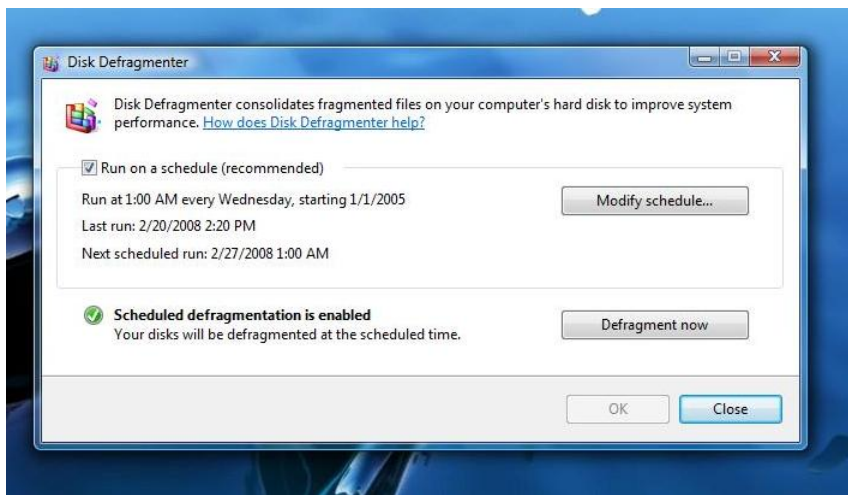


Figure 1. Screen shot of defragmentation in Vista

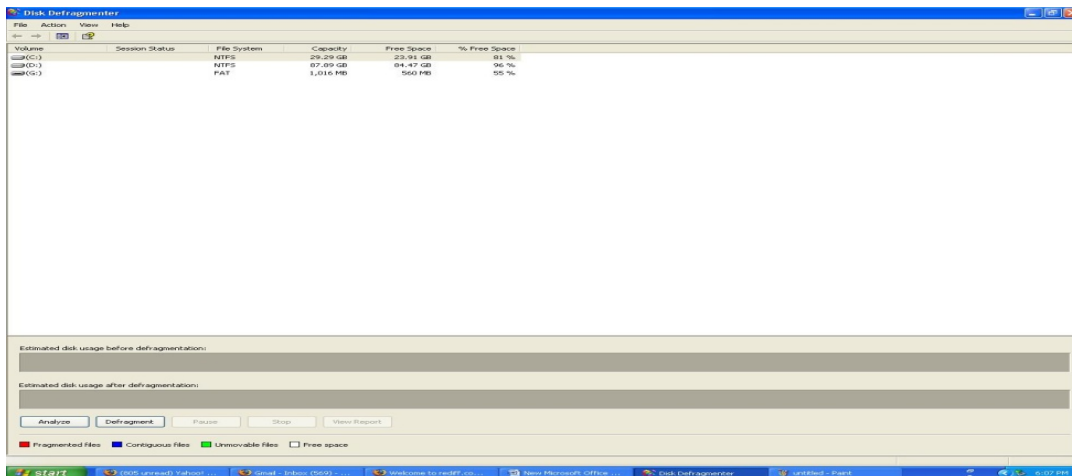


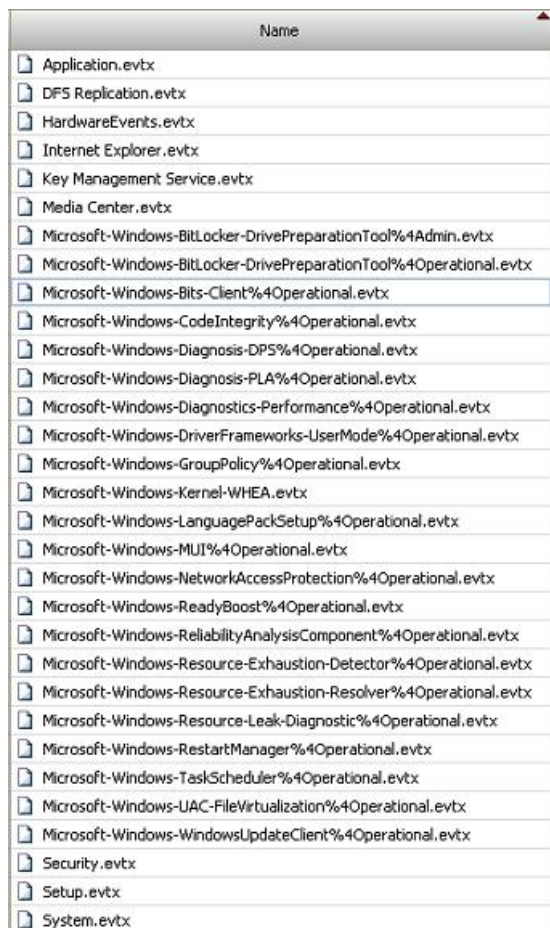
Figure 2. Screen shot of defragmentation in Windows XP

B. Event Logs

Windows event logs have changed dramatically in Vista. A new XML file format is being used for the event logs and a new extension of “EVTX” is now used. The files are now located in:

- “C:\Windows\System32\winevt\Logs\”

There are now approximately 30 different event logs that Windows Vista reports events to. Currently these logs can only be read by the native Windows Vista Event Viewer (eventvwr), although an EnCase EnScript is under development. Below is the screen shot of Event Log of Vista (Lance, 2007).



The screenshot shows a window titled "Name" with a list of event logs. The list includes:

Name
Application.evtx
DFS Replication.evtx
HardwareEvents.evtx
Internet Explorer.evtx
Key Management Service.evtx
Media Center.evtx
Microsoft-Windows-BitLocker-DrivePreparationTool%4Admin.evtx
Microsoft-Windows-BitLocker-DrivePreparationTool%4Operational.evtx
Microsoft-Windows-Bits-Client%4Operational.evtx
Microsoft-Windows-CodeIntegrity%4Operational.evtx
Microsoft-Windows-Diagnosis-DPS%4Operational.evtx
Microsoft-Windows-Diagnosis-PLA%4Operational.evtx
Microsoft-Windows-Diagnostics-Performance%4Operational.evtx
Microsoft-Windows-DriverFrameworks-UserMode%4Operational.evtx
Microsoft-Windows-GroupPolicy%4Operational.evtx
Microsoft-Windows-Kernel-WHEA.evtx
Microsoft-Windows-LanguagePackSetup%4Operational.evtx
Microsoft-Windows-MUI%4Operational.evtx
Microsoft-Windows-NetworkAccessProtection%4Operational.evtx
Microsoft-Windows-ReadyBoost%4Operational.evtx
Microsoft-Windows-ReliabilityAnalysisComponent%4Operational.evtx
Microsoft-Windows-Resource-Exhaustion-Detector%4Operational.evtx
Microsoft-Windows-Resource-Exhaustion-Resolver%4Operational.evtx
Microsoft-Windows-Resource-Leak-Diagnostic%4Operational.evtx
Microsoft-Windows-RestartManager%4Operational.evtx
Microsoft-Windows-TaskScheduler%4Operational.evtx
Microsoft-Windows-UAC-FileVirtualization%4Operational.evtx
Microsoft-Windows-WindowsUpdateClient%4Operational.evtx
Security.evtx
Setup.evtx
System.evtx

Figure 3. Vista Event log

WinHex and X-Ways Forensics have confirmed that if a file in an NTFS volume has only been partially filled with data then these files are marked with "partial init." (partial initialization) in the Attribute column. The size of the actually initialized/defined portion of the file is now displayed in the Details Panel when opening such a file or when looking at it in File mode, labeled as "Valid data length", and the affected uninitialized range will be displayed in a different color. Search hits in the uninitialized portion of a file will be marked as search hits in "slack etc". The fact that a file has been partially initialized only will also be remembered by containers. All of that is meant to help a skillful forensic examiner to avoid drawing inaccurate conclusions. This risk exists because data that is stored in the

allocated clusters of a file may be old data that was present on the disk before the clusters were allocated to that file, if the clusters have never been actually overwritten with new data. In other words, there may be data that has nothing to do with the file, although according to the logical file size it is part of it (Carvey, 2006). File types that are not always fully initialized can include Windows Registry and Windows Event Log (.evtx). Event logs are important to investigators who may try to build up a portrait of a suspect's behavior. For example, viewing the event logs for a computer would be critical for a case involving Internet Chat, especially when trying to prove that an individual was communicating at certain times. The event logs would also be important to determine if a suspect had attempted to secret information or tamper with evidence.

C. Windows Search Engine (Indexing)

Windows Vista includes a new search engine and indexing feature. Indexing has been available since Windows 2000 but it was turned off by default (Carrier B. , 2005). In Windows Vista, it is enabled by default. The new search feature is accessible from the *Start Menu* or any Windows Explorer window (Lance, 2007). Users can now save their searches and review the results in real-time as the search results are updated as new files are added to the system. Saved searches are placed under the user's profile:

- C:\Users\\Searches

The indexing service is used to quickly locate files by indexing the file's metadata and contents (some file types). Microsoft Mail is included in the types of data that is indexed and available for searches. These indexes are located in the following location:

- "C:\ProgramData\Microsoft\Search\Data\Applications\Windows\Projects\systemIndex\Indexer\Ci Files"

Vista maintains several index files in this directory and these can be searched for keywords using the keyword search feature in EnCase. When extracting e-mail messages and attachments, attachments now become child objects of their respective parent e-mail messages. That makes it very easy to find the attachments for a given e-mail message, or to find the e-mail message that contains a given attachment. Because of this parent-child relationship, one can now conveniently include the containing e-mail message when copying attachments to evidence file container, or include the attachments when copying the e-mail message. Tagging an e-mail message will also tag its attachments. Tagging an attachment will at least partially tag the containing e-mail message (Garfinkel, Febraury 2006).

The logs for Refine Volume Snapshot, Logical Search, and Indexing, which contain the internal IDs of processed files to identify the offending file in case of a crash, are no longer stored in separate log files and no longer in the evidence object metadata directories. Instead, a single file "VS.log" is now created in the directory from where X-Ways Forensics is run, and it is overwritten each time a new operation is started. This means you no longer have to search for the correct log file for the last operation, and it also saves drive space. As before, the last line in such a file specifies the internal ID of the last file that was processed.

Unlike many other aspects of Vista, the new default settings for indexing are a boon to investigators trying to ascertain ownership, intent and control by a suspect.

D. ReadyBoost and Physical Memory

ReadyBoost is a Microsoft feature which allows a user to add virtual memory by using a removable flash drive. This memory is then cached and used as an extension to installed physical memory. Flash memory is much faster than paging data to the *pagefile* on a hard disk and is therefore a cheap alternative to adding memory to a system.

Data that is written to the removable flash disk is encrypted using AES-128 encryption before being written to the flash disk. Therefore an examiner who recovers a flash disk used for ReadyBoost will not be able to decipher the data.

Accessing physical memory using DD is a common way of collecting volatile data (contents of RAM) before a system is shutdown and/or imaged. This procedure works in Windows 2000 and Windows XP but does not in Windows 2003 and Windows Vista. This is because the \\.\PhysicalMemory Pipe is not accessible even from an administrator account. Therefore, it is currently not possible to collect physical memory using the standard version of win32 DD.EXE. ReadyBoost is an important feature for an examiner to be cognizant of, especially because USB memory has become so pervasive in recent times and it can now be used as an extension of a system's volatile memory and the file footprint for a USB drive has changed with Vista.

E. File Metadata

The last access dates in Windows Vista are no longer updated when a file is accessed. Microsoft explains that with all the new file system transactional journaling, it was somewhat of a performance hit, so they have disabled them by default.

Name	Last Accessed	File Created	Last Written
Videos	02/27/07 02:16:14PM	02/27/07 02:15:11PM	02/27/07 02:16:14PM
Downloads	04/15/07 01:24:59PM	02/27/07 02:15:11PM	04/15/07 01:24:59PM
calc.exe	04/15/07 01:22:41PM	04/15/07 01:22:41PM	11/02/06 05:32:43AM
Contacts	02/27/07 02:15:39PM	02/27/07 02:15:39PM	02/27/07 02:15:39PM
Favorites	02/27/07 02:16:22PM	02/27/07 02:15:11PM	02/27/07 02:16:22PM

Figure 4. File Metadata Represented in Vista

In Windows Vista, this feature is enabled by default. This feature can be turned off via a registry key. This default setting obviously has a severe impact on how some types of cases are analyzed and examiners should take great care when using these date stamps as part of their analysis (Disabling last access time in windows vista to improve ntfs performance, 2006). A reduction in file metadata is a serious blow to criminal investigations. For example, it is not enough to simply find contraband images stored on a suspect's computer, facing child endangerment charges. Intent must also be demonstrated, by the prosecution, with accurate information pertaining to file access times.

F. Volume Shadow Services

The Volume Shadow Service was first introduced in Windows XP in a limited way and then further enhanced in Windows 2003 Server. Its goal was to create copies of important files that could then be

safely backed up without having file locking issues. It was off by default and only a limited number of files or directories could be shadowed in Windows 2003.

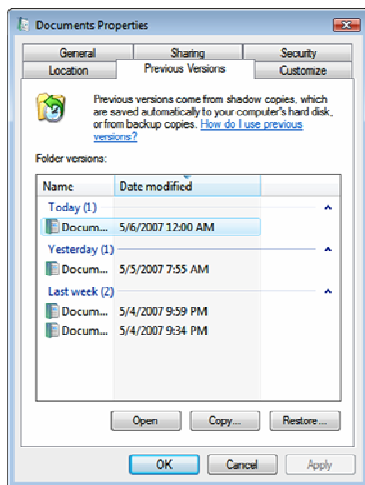


Figure 5. Volume Shadow Copy Program in Vista

The block level changes that are saved by the “previous version” feature are stored in the System Volume Information folder as part of a restore point. This data is not encrypted (absent BitLocker) and can be easily searched using the EnCase search feature. In the root of the “System Volume Information” folder, several files can be seen with GUIDs as the filename (Lance, 2007).

	Name
<input checked="" type="checkbox"/> 1	MountPointManagerRemoteDatabase
<input checked="" type="checkbox"/> 2	{b9fca579-fac4-11db-94e1-000c29471bd4}{3808876b-c176-4e48-b7ae-04046e6cc752}
<input checked="" type="checkbox"/> 3	{3808876b-c176-4e48-b7ae-04046e6cc752}
<input checked="" type="checkbox"/> 4	{aa7164c3-faac-11db-b913-000c29471bd4}{3808876b-c176-4e48-b7ae-04046e6cc752}
<input checked="" type="checkbox"/> 5	{003186d8-fb18-11db-9974-000c29471bd4}{3808876b-c176-4e48-b7ae-04046e6cc752}
<input checked="" type="checkbox"/> 6	{4f4b3220-fb3b-11db-8172-000c29471bd4}{3808876b-c176-4e48-b7ae-04046e6cc752}
<input checked="" type="checkbox"/> 7	SPP
<input checked="" type="checkbox"/> 8	tracking.log

Figure 6. Saved Block Level Changes in Vista

II. CHANGES IN EVIDENCE

Log files are generally an important source of information in a forensic examination. The new log file format consists of a small file header, which is followed by a series of chunks. The chunks are self-contained. No event record will extend over the boundary between two chunks. Thus, for every event log only the current chunk (64 KB) and the file header (4 KB) have to be mapped into memory. Events are in XML but are encoded in BXML. A practical test was conducted in the forensics laboratory, at Pace University, on Windows XP and Vista. The experiment hypothesized that a person wanted to change the system time after committing the crime. It was possible in both operating systems but the nature of the evidence is different in Vista’s Event Viewer compared to that of Windows XP. The Vista Event Viewer

clearly shows that the system clock was manipulated while The XP Event Viewer showed no record of the system clock being changed. This experiment was important because accurately determining a series of events in a criminal investigation can be critical. Thus, Windows Vista Event Viewer can potentially provide better evidence to a forensics investigator than previous versions of Windows. Below is the screen shot from Vista and it is compared with XP.

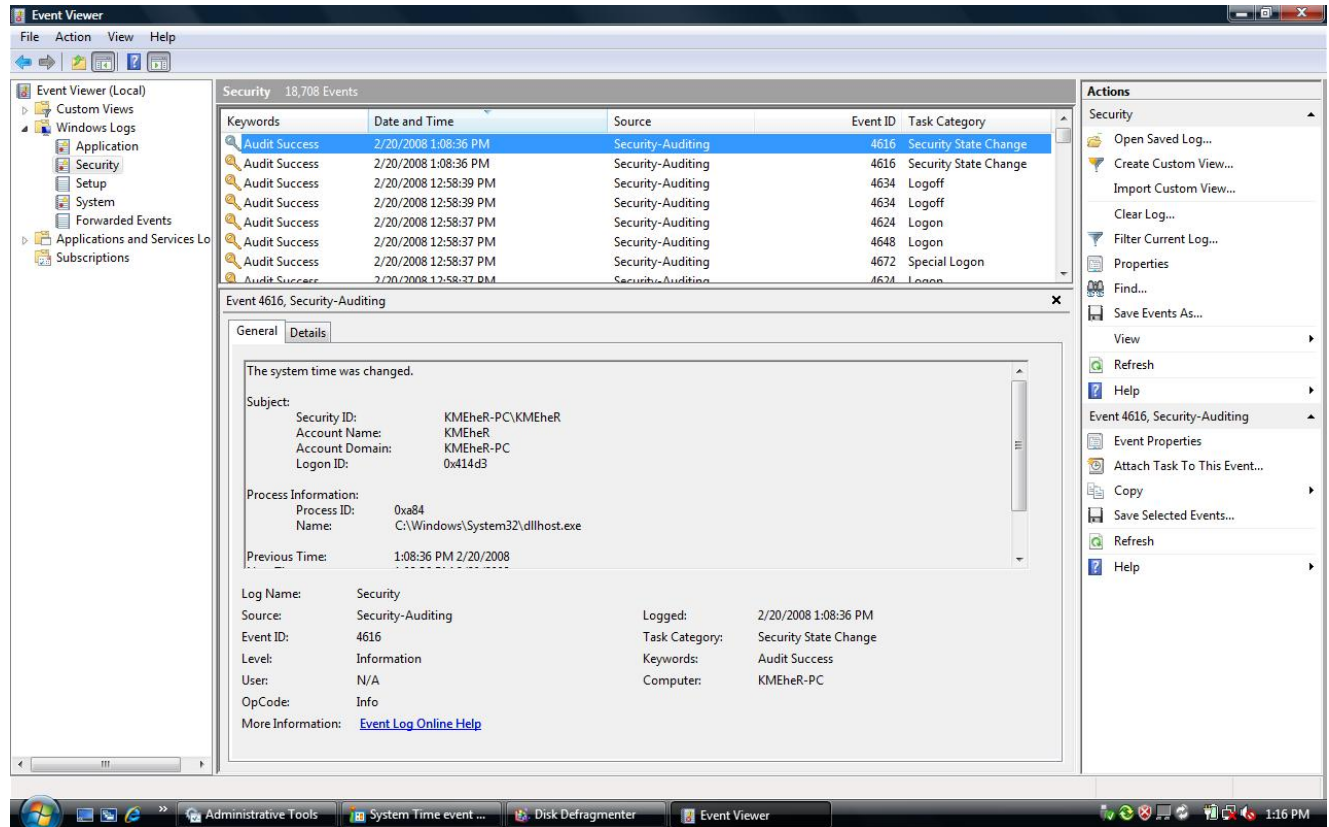


Figure 7. Windows Vista Event Viewer

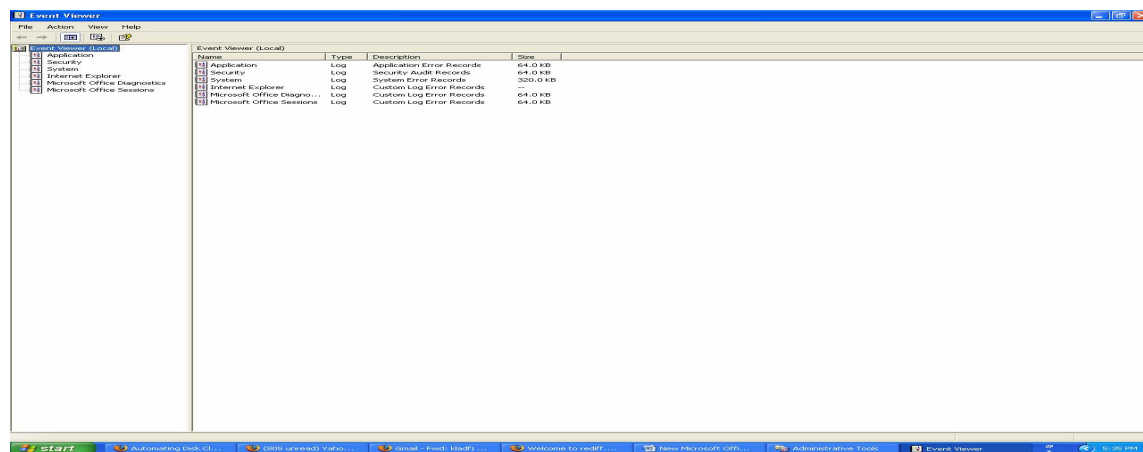


Figure 8. Windows XP Event Viewer

III. CONCLUSION

Windows Vista can be viewed as more problematic for investigations involving the use of digital evidence. The problems encountered are mainly as a result of enhancements made to encryption, through Vista's Encrypted File System (EFS), BitLocker Drive Encryption with Trusted Platform Module (TPM) and electronic mail encryption in Windows Mail (Hayes & Qureshi, 2008). For the purposes of this paper, it appears evident that Microsoft has sought to remove the user from many housekeeping tasks associated with operating systems, such as file restoration and defragmentation. On the one hand, Shadow Copy and file restoration features will be beneficial to examiners. On the other hand the introduction of automatic defragmentation poses new problems for data recovery. Vista is dramatically different and computer forensics investigators will need to adapt to changes in the nature of evidence, its value as well as new methods of retrieval.

REFERENCES

- A. Andreas, S. (2007, August). *A parser to transform vista event log files into plain text*. Retrieved from http://computer.forensikblog.de/en/2007/08/evtx_parser.html
- B. Baryamureeba, V. a. (2007, November). *The Enhanced Digital Investigation Process Model*. Retrieved from www.dfrws.org/2004/day1/tushabe_EIDIP.pdf
- C. Berghel, H. (2007). *Hiding Data, Forensics and Anti-Forensics*.
- D. Carrier, B. (2005). *File System Forensic analysis*. Upper Saddle River, NJ 07458: Addison-Wesley.
- E. Carrier, B. (2005). *File System Forensics Analysis*. Addison Wesley.
- F. Carvey, H. (2006). *Windows Forensics and Incident Recovery*. Addison-Wesley.
- G. Disabling last access time in windows vista to improve ntfs performance. (2006). blogs.technet.com/filecab/archive/2006/11/07.
- H. *File Extensions*. (2005, September). Retrieved from www.filetext.com/harmful.htm
- I. Garfinkel, S. (February 2006). *AFF: A New Format for Storing Hard Drive Images*.
- J. Hayes, D. R., & Qureshi, S. (2008). *A Framework for Computer Forensics Investigations Involving Microsoft Vista. LISAT*. Farmingdale: IEEE.
- K. John, M. (2007, October 23). *Finding the user setting in Vista*. Retrieved February 3, 2008, from www.devsource.com/article2/0,1895,19996337,00.asp
- L. Lance, M. (2007). *Basic Investigations of Windows Vista*.
- M. Microsoft. (2007, September). *Description of the Microsoft Windows Registry*. Retrieved from <http://support.microsoft.com/default.aspx?scid=kb;EN-US;256986>
- N. Microsoft. (2007). *Microsoft's Windows OS global market share*. Retrieved from http://www.onestat.com/html/aboutus_pressbox10.html
- O. Microsoft. (2002, November 2). *MSDN*. Retrieved January 2008, from <http://msdn2.microsoft.com/en-us/library/ms715237.aspx>