SOLID STATE DISK FORENSICS: IS THERE A PATH FORWARD?

by

John William Fulton

A Capstone Project Submitted to the Faculty of

Utica College

May 2014

in Partial Fulfillment of the Requirements for the Degree of

Master of Science in Cybersecurity

Abstract

Solid State Disks (SSDs) are reaching the point of being a practical replacement for traditional spinning media hard disk drives. With no moving parts and containing only semiconductor memory components, SSDs are faster and more reliable than spinning media drives but carry a price and size penalty. While the forensic analysis of the contents of spinning media drives is well understood and legally accepted, the increased complexity and autonomous actions of SSDs create serious challenges to the reliability of analysis on such devices. The limited lifespan and the slow erase times for blocks of memory have caused manufactures to create behavior that eliminates most forensic artifacts from unallocated space. Because of the autonomous actions of these intelligent devices, forensic analysis can produce different results in the absence of any user initiated changes. In a limited number of cases, data may still remain in an SSD's unallocated areas, but examiners should continue to focus on the allocated files and the rich set of information left behind there.

Keywords: Cybersecurity, Christopher Riddell MS, digital forensics, solid state drives, forensic analysis, wear-leveling, pre-clearing.

Acknowledgements

My profound thanks to my family and friends, especially my loving wife Lisa, who have put up with my long nights and weekends of focus on my class work and this paper. Their support, kind words, and tolerance have made this experience far easier. My second reader, James Lewis of Cyber Defense Training Systems has contributed immensely to the breadth and depth of this paper with his suggestions and encouragements. I appreciate the efforts and guidance of my faculty members at Utica College, especially those of Jeff Bardin and Vern McCandlish who both breathe real live and excitement into their subjects. Much credit goes to Chris Riddell and Jay Lopez for the help and guidance through the capstone process. Their suggestions and guidance have been a substantial factor in my success and that of the other students in my cohort. I would also like to express my sincere thanks to my employer Grange Insurance and my manager Bob Reid for their material and moral support.

I dedicate this paper to my children; Timothy, Lauren, Fritz, and Chris. My hope for them is that their lives will be as rich and full as I have found mine to be.

Table of Contents

Solid State Disk Forensics: Is there a path forward?

Since the earliest appearance of advanced Solid State Disk (SSD) devices, the challenge of providing digital forensic access has been apparent. Traditional computer forensic examination of stored data is facing many challenges but the growing adoption of SSD is being called "the beginning of the end for current practice in digital forensic recovery" (Bell and Boddington, 2010, p. 1). Traditional spinning media disk drives leave behind a rich set of artifacts that examiners have come to depend upon to recover recently deleted files and to search for fragments of long deleted files. As independent intelligent devices, SSDs do not leave behind the artifacts previously found on spinning media devices.

Currently about 6% of the total disk drives shipped each year are SSDs (Kingsley-Hughes, 2013). It is projected that over 20% of all new disk devices will be SSDs by 2016 (StorageNewsletter, 2014). Although much of the growth is in laptop and netbook computers there is increasing interest in the price/performance and overall advantages of SSDs for desktops and servers (Narayanan, Thereska, Donnelly, Elnikety, & Rowstron, 2009).

An extensive body of commercial and open source tools have come into use to provide examiners with the ability to recover many types of information from spinning media disk drives, including the contents of memory swap files, fragments of deleted disk files and even complete (or mostly complete) files. Several authors have provided rich details of the limitations and restrictions imposed upon forensic examiners by SSD technology (Antonellis, 2008; Bell & Boddington, 2010; Burnett, 2012). A few have proposed technology responses (Bednar & Katos, 2011; Gubanov & Afonin, 2012). None of these proposals have been widely adopted and the number and type of SSD devices continues to proliferate.

The purpose of this research was to examine the limitations on SSD artifact recovery. Does the technology of SSDs place inherent limitations on the recovery of artifacts of deleted files? What role do the decisions of manufactures and the marketplace play in the difficulty of recovering forensic artifacts? Are there advances in standards or technology that are likely to improve this situation?

SSDs are direct, plug compatible replacement devices for the spinning hard disk drives that provide most of the persistent storage of data and programs in modern computers at the laptop scale and above. SSDs are faster, lighter, and more reliable than spinning media drives. Spinning disk drives are cheaper and offer more storage in the same package size. Through the use of a separate processor, memory, and software, SSD devices emulate the function of a spinning disk drive to the operating system of a server, desktop or laptop computer. The emulated function of the spinning media drive is provided in the software and solid state hardware of the SSD device.

Spinning magnetic media were one of the first methods used to store information in electronic digital computers. Spinning magnetic drums were used as early as the 1940's (Da Cruz, 2001). Disk storage first appeared in the 1950s (Computer History Museum, 2012). From the beginning, compromises were necessary to increase the efficiency of storage and retrieval operations. Some of these compromises, especially concerning the partial erasure of deleted files, has provided a rich field of play ever since for the recovery of these partially erased files by forensic analysts.

In general, from the earliest storage schemes, a table of the files stored on the disk was kept separately from the actual storage space. This file allocation table provided the keys to the location of the actual data on the disk. One efficiency that was adopted almost universally was that to erase a file, it was necessary only to remove the appropriate entries in the file allocation table, removing the links to the data on the disk. No links equated to no data. Forensic analysts quickly discovered that it was possible to recover much or all of the contents of a “deleted” file by examining the contents of the disk for the not-yet-reused areas on the disk that still contained the data from the deleted file. Because of the structure of the data, it was often possible to recover all or most of files – especially ones that had been recently deleted. At least some fragments of deleted files were almost always present.

With the development of the Universal Serial Bus (USB) in the mid-1990s (Garfinkel, 1999), a convenient interface became available for the introduction of a rugged, portable, persistent memory device with no moving parts, the flash memory drive. Although they are not moving disk memory devices, to ease interoperability with existing operating systems and application programs, the computer software that communicates to the hardware “sees” the flash drive as if it were a spinning media drive, with a file allocation table and clusters just like a spinning media drive (Microsoft, 2000). The hardware in the flash drive converts those commands sent by the computer to appropriate commands for its different style and type of storage.

Because flash drives are a persistent storage device, reliably retaining their data for extended periods with no electrical power, the choices for hardware to provide the memory technology are limited and provide some unique challenges for the designer. Only a few types of commercially available semiconductor devices provide the ability to easily and quickly read and write and yet provide the reliable storage with no power consumption or active refresh circuitry. The technologies used impose limitations on the way data is written to the devices, most notably in the large block sizes, and provides a limitation on the number of times that the same area of memory can be written and re-written. The limit varies based on the technology and manufacturing techniques from a few thousand to hundreds of thousands of read/write cycles. This compares to millions of read/write cycles for traditional spinning media devices. As temporary devices, USB flash drives are less likely to encounter these read/write limits than they would as permanently installed, full-time storage devices. These hardware characteristics play a major role in the nature of the forensic artifacts left behind during their use.

SSD devices as a plug compatible replacement for spinning media drives are a direct successor to the precursor flash drives, with larger storage, more complex controller hardware and firmware, and a form factor that allows them to replace traditional spinning media drives. The use of SSD devices continues to grow rapidly as the adoption of the technology spreads. The legacy spinning media disk technology that SSD is replacing has become a commodity (Mckendrick, 2001) and further improvements in density or price/performance are unlikely (Rosenthal, Rosenthal, Miller, Adams, Storer, & Zadok, 2012). SSD has a great deal of appeal for persistent storage in many types of devices because of its shock resistance, faster access and transfer times and lower latency (Deng, 2011).

As the cost of solid-state memory continues to decrease based upon Moore’s Law (Li & Yang, 2007), SSD is an increasingly attractive general purpose replacement for spinning media disks in desktop and laptop computers (Narayanan et al., 2009). Narayanan & Thereska further suggest that as the price/performance of SSD continues to improve, large scale server arrays of spinning disk media are becoming an increasingly attractive target for replacement with SSD. Several semiconductor technologies have been commercially developed that fall under the banner of SSDs and those details are discussed in depth elsewhere (Freitas & Chiu, 2010).

As more devices incorporate SSD as a primary storage device, forensic examiners are increasingly confronted with their inability to examine the SSD devices for anything other than the currently existing files defined in the directory of the SSD and the connected device (Bell & Boddington, 2010). SSDs, because of the nature of their storage of information, write and erase data in very different ways from spinning media disk drives and this leads to very different results when users delete files from an SSD-based file system (Ekker, Coughlin, & Handy, 2009). Traditional methods of dead-box forensics against SSDs removed from computers under examination will yield far fewer forensic secrets than spinning media disk drives.

SSDs are intelligent devices with a separate general purpose computer and stored programs of their own to emulate the operations and formats of traditional spinning media drives. Among other autonomous actions, SSDs implement rewriting of files to different physical locations on the SSD to prevent the same block in semiconductor memory from being written over and over again. This “wear-leveling” technique is used widely (although not universally) in SSD implementations. This wear-leveling causes a file that is partially re-written to have sections of the file written in many different, random locations in the storage area. This is different from the technique used with traditional spinning media drives where a file being partially re-written would be written to the same area of the disk over and over. This wear-leveling technique in most SSDs spreads writes over the entire storage area. It increases the chance that parts of previously deleted files will be written over, decreasing the chances of finding parts of deleted files in subsequent forensic analysis.

In contrast with the traditional spinning media disk drives which only require the target sector to be rewritten when changed, most SSD technologies require that blocks be initialized to a pattern of all binary ones or zeros prior to writing a block (Bell and Boddington, 2010). In the case where there are many blocks to write, this “clear” activity can substantially decrease the throughput of the SSD device. Many manufactures have elected to increase the effective throughput of their SSD device by doing pro-active *garbage collection* and initializing unused blocks of storage when no other operations are going on. These garbage collection activities are based on the information that the SSD stores in its equivalent of the file access table, causing the device to initialize the segments on the SSD that were previously occupied by portions of files that have been re-written elsewhere for load-leveling or that have been deleted. Once these areas of data have been rewritten and initialized for use, the data they previously contained is no longer available for forensic analysis. SSD garbage collection is a substantial and difficult issue for forensic analysis of SSDs.

Unlike traditional spinning media drives, just powering up an SSD, even one that has been removed from the computer, can allow the garbage collection routines on the SSD to continue. These pre-clearing actions forever alter the data on the drive and its value as evidence. In most cases there is no way for the garbage collection or load leveling functions to be disabled.

There is a lack of tools specifically geared to extracting evidence from SSDs in a forensically sound manner. Conventional techniques lack the forensic certainty of traditional disk drive techniques. They continue to be used despite the limits of those technologies and the risk of incompleteness. The lack of tools is such a serious problem that the Department of Homeland Security launched an effort to find practical methods of extracting information from SSDs in a forensically sound fashion and to develop tools that implement such methods (Cooney, 2012).

Several suggestions are offered for dealing with SSDs in a forensic setting, mostly centered on getting the data off the drive and powering off the drive as quickly as possible if the information extraction needs to be delayed (Sheward, 2012). Because of the wide variety of technologies used to construct SSDs and the closed and proprietary nature of the hardware and algorithms used to provide for rewriting files and wear-leveling, one of the greatest limitations to forensic examination of the technology is the secrecy surrounding the details of operations on the storage areas. Although there have been efforts to provide interface standards (SNIA, 2014) there is no requirement of manufactures to follow the standards, especially access to the semiconductor flash memory where the two largest manufacturers, Samsung and Toshiba (Yinug, 2007) are not a part of the industry group that is promoting the standard.

Each of the manufactures seeks competitive advantage in the market place to provide for faster access, greater throughput, lower cost, and a greater number of read/write cycles in a fast evolving marketplace. This has resulted in an explosion of technologies, algorithms and methods for storage, wear-leveling, garbage collection and buffering within the devices. The forensic examiner is faced with a large number of mostly proprietary and protected technologies that act on the data based on the commands of a separate computer and stored programs that make up the SSD.

Assuming the continued acceptance of SSDs to replace spinning media drives, the job of forensic analyst will continue to increase in complexity and the historic artifacts of deleted but not erased files left behind on persistent storage devices may no longer be available. If there are productive paths forward toward forensic analysis of SSD devices, then such paths would yield rich rewards in law enforcements, data recovery (Pal & Memon, 2009) and other disciplines. If, despite the best efforts of researches and developers, there are no productive paths to follow in the forensic analysis of SSD devices, then such research can be set aside to explore more productive undertakings.

Literature Review

Spinning Media Drives and File Storage

Early in the history of computing, the value of persistent storage was apparent. In his classic work on computability, Turing (1936) described a conceptual “tape” that stored symbols in cells that were acted on by the tupples that described the actions of his machine. Early commercial computers included spinning magnetic drums (Da Cruz, 2001) that provided access to blocks of digital data that could be written and read randomly, that is they could be read and written in any order that was useful to the computer program being executed, not just in a linear sequence. The drum storage removed the requirement that data be read from external storage from the beginning until the desired block was found but also allowed the changing of data on the storage media by re-writing a track (Podlipnig & Schnhart, 2014; Thomas, 1998). This random organization of data on magnetic drums mapped data to bands or tracks of encoded material on the drum, each of which contained distinct information. These tracks were later divided into sectors, each track on the drum containing several sectors (General Precision, 1964). Buffering circuitry in the magnetic drum drive provided the ability read, write and over write specific sectors under program control.

The introduction of spinning platter drives replaced the spinning drum with spinning disks of magnetic media. The disks were formatted with multiple concentric tracks replacing the parallel tracks of the magnetic drum (IBM, 2014). The sectors continued to provide readable and writable subdivisions of the tracks on the platters as they had on the drums. From the earliest drives, a moving read/write head for each platter allowed the reading or writing of any sector or grouping of sectors (cluster) with some delay for the movement of the head to the correct track (seek time) and some delay for the sector or first sector of the cluster to rotate under the read/write head (rotational latency) (PCtechguide, 2011).

As the amount and types of data stored on magnetic media increased and the size of the media increased, it became increasingly important to provide for organization schemes that tracked the allocation of sectors on the disk to the stored programs, parameter files, and user data files that they represented. Early file systems approached the problems in a number of ways (Arpaci-Dusseau, 2014), but many included some form of a file allocation table that provided identification of the file, ownership, and permission information. Along with this metadata about the file, the file allocation table also contained an index or pointer to the first cluster of the data contents of the file on the spinning media disk (Lsoft Technologies Inc., 2014). A small amount of space at the beginning of each sector was allocated to indexes or pointers that would link to the next sector being used for the file. The last sector of the file provided an indicator. This linked list of sectors constituted the data portion of the file. When a file was accessed, the controller hardware and software worked together to lookup the desired file in the file allocation table and then follow the chain of linked sectors to retrieve the file for the use of the requesting program.

When a file was no longer needed on the disk, one approach would be to start at the file allocation table and find each of the sectors that was allocated to the file and then overwrite the areas of the disk allocated to the file. This method is available and tools exist for most environments that implement such a scheme (Kaufman, 2011) but it is not in general use for spinning media disks. A method that is far faster and creates less wear and tear on the disk drive is the industry practice of altering the file allocation table to mark the file as deleted and no longer available for general access. Some operating environments show the entire file in a recycle/recovery area (Microsoft, 2014b), while others mark the linked list of sectors available for re-use by another program looking for available disk space. In any case, it is the ordinary and normal practice in the industry to leave deleted files largely intact, awaiting un-deletion by the user who discovers a file was deleted in error or recovery by a forensic tool that can, with or without the availability of the file allocation table, follow the chain of sectors that made up the data portion of the files.

Early disk drives provided responses to read requests in an average of approximately 25 milliseconds (General Precision, 1964). Although substantial improvements have continued in engineering and materials, spinning media drives are still limited by the physics of mass and motion. Deng (2011) found that modern spinning media drives had seek times of approximately 3.5 milliseconds and rotational latencies that averaged 2 milliseconds, approximately 5 times faster than the earliest disk drives.

Forensic Investigation of Spinning Media Drives

Forensic investigators are focused by a few key principals when examining spinning media drives. They are guided by a Hippocratic-like oath of “doing no harm”, that is, to preserve the integrity of the original media, allowing nothing to be written to it, making a complete back up as soon as possible and only performing analysis of that forensically sound copy. In dead box forensics, the primary focus of the digital forensic field until about 2005 (Adelstein, 2006), the forensically sound copy is the holy grail, and most open source and proprietary tools are focused on creating forensically sound copies and performing analysis of them,.

Once a copy exists, many types of analysis are possible. Once the file system has been identified, the currently allocated files can be listed, enumerated, searched, hashed, and cataloged. The allocated files would include all of the files and directories that would exist for the user within the computer’s operating system or application programs. They would include all of the files loaded onto the disk when the operating system and other software were loaded. They would also include all the configuration files generated from setting parameters within the operating system and other software and the log files generated by those programs. Also included would be all of the files created and downloaded by the user including many temporary files created as intermediate files by working with software, reading web pages, and other actions by a user. Most users only become aware of the number of files on their computer when running a full scan or backup, realizing that they have tens of thousands of files on their quite ordinary desktop or laptop.

Information not within the current allocation of files on spinning media drives can also be recovered to a greater or lesser extent. Forensic analysis can provide complete information about files that have been marked for deletion but remain allocated within the file system. In current versions of the Windows operating systems, such files are allocated to the recycle bin and can be recovered to their original location by user interaction through the graphical user interface. Files that have been deleted from the recycle bin in the Windows paradigm or truly deleted can still be recovered even if no file allocation table information remains through a process called file carving. Most different types of files have characteristic patterns of characters or bits that identify the beginning of the data portion of the file (Kessler, 2014) and knowledge of those patterns along with the ability to follow the chain of allocated sectors on the spinning media disk allows many forensic tools to reconstruct the data portions of files even in the absence of metadata. This classic method of spinning disk forensics is dependent on how much other data has been written to the disk since the file was deleted. Any disk sectors that are reused for some other file would break the chain of sectors and would result in a partial file being found in the file carving of the disk.

Another component of the analysis of spinning media drives is the ability to do fragmentary analysis. Such analysis can allow the examination of a chain of segments without an identifiable header, individual isolated sectors that are not part of a chain, and slack space analysis. Slack space analysis depends upon the difference between the space available to a program in a sector and the amount actually used by the program. In most programs, the allocated but unused space in the sector of the spinning media drive is left untouched, retaining whatever data was in the sector prior to its reallocation.

Taken together, these intended and unintended sources of data on a traditional spinning media drive provides a rich field for exploration by forensic analysts. Commercial product suites such as Encase, Forensic Toolkit (FTK), and others provide tools to capture data from a disk to a forensically sound format, examine the data based on the file allocation table, carve data based on file signatures, and to search the data for human readable characters in a variety of character sets (the so-called “printable” characters). It is also possible to search using these commercial tools for a specific character string or for characters matching specific pattern, for example, a phone number, an email address, or a credit card number. A large number of open source tools, especially running in the open-source Linux environment, are also available to analysts to perform similar capture and analysis functions. Commercial and open source tools are both widely used and accepted as accurate methods of understanding the contents of spinning media drives.

Solid State Disks

The advent of the USB as a standard for relatively high transfer rate serial devices in 1995 (Seebach, 2005), provided an attractive target for the use of semiconductor memory as a portable storage medium. The first USB external storage devices appeared in 2000 (Ban, Moran, & Ogdan, 2000) and modeled the behavior of the spinning media hard disk drives and floppy disk drives that proceeded them. By today’s standards, the first drives had a relatively low density at 8, 16, 32 and then 64 megabytes and a high cost per megabyte of storage at about $1 per megabyte (Microcenter, 2001). In early 2014 it is possible to purchase USB flash drives for $0.50 per gigabyte and in densities up to 128 gigabytes (Newegg, 2014).

USB flash drives were the precursors of the SSD drives that offer plug compatible replacement for traditional spinning media drives. In addition to the mechanical USB connector and packaging, the USB flash drive consists of two collections of electronic devises on a single printed circuit board. The first set of components is the simplest, comprising a memory chip or chips that provide for storage of the information encoded on them.

A few requirements dictate the semiconductor technologies available to the designer of such devices. The devices have to draw a limited amount of power when being read and written. Read and write cycles have to be short enough to meet users expectations for storage operations and the devices must reliably store the information written to them when power is removed. The semiconductor technologies are characterized by the binary logic employed in their construction. Devices using the Boolean NOR (Not OR) logic (Basic Electronics Tutorials, 2014b) are designated as NOR flash memory. NOR flash memory is characterized by a lower density due to the presence of additional connections that provide addressability at the byte level (Masuoka & Iizuka, 1985). The most commonly used technology in USB flash drives is characterized by the

Boolean NAND (Not AND) logic (Basic Electronics Tutorials, 2014a). NAND technology is preferred because of its high density, but this is achieved by providing fewer connections for addressability (Masuoka & Iizuka, 1985). The result is that NAND flash memory is only addressable to the block level, in blocks of 512 bytes and often larger (Kim, Kim, Noh, Min, & Cho, 2002).

The other major set of components of USB flash drives is the electronics and firmware package on the devices that allows the device to appear to the external computer that the flash drive actually is a disk drive, with the expected sectors and clusters. In reality, of course the flash drive has none of these; the controller electronics and firmware provide a simulation of those organizations of data in response to operations sent over the USB connection. This set of controller electronics has become more sophisticated over the years, beginning as a way to map the actual solid state storage to the appearance of disk clusters for the attached computer (Ban et al., 2000) and evolving to provide a flash translation layer (Kim et al., 2002) to provide the mapping. As the sophistication of the controller electronics and firmware continued to increase, manufactures sought to increase the lifespan of the devices.

A limitation of the NAND flash memory is the number of write cycles in the lifetime of each block. Because of the manufacturing technology, NAND flash memory can only be written a block at a time (Masuoka & Iizuka, 1985) and each block can only be written for 100,000 to 1,000,000 times (Micron Technology, Inc., 2008; Thatcher, Coughlin, Handy, & Ekker, 2009) As the manufacturing technologies have improved the number of write cycles continue to increase, but this is still substantially below the predicted lifespan of current-generation spinning media disks in excess of 1.3 million hours (White, 2011). To combat the limitation of a shorter lifespan of data blocks, manufacturers provided deliberately unused “spare” blocks that could be substituted for failed blocks and instituted a process of “wear-leveling” where a specific block being re-written or altered would not be re-written at its original location, but rather at a different physical location in memory. A block of memory that was re-written frequently would be written to many different positions in memory to lessen the chance that the block would induce more *wear* on one specific memory location. As the complexity of the processing required for the replacement of blocks with errors and the re-mapping of the virtual disk sectors and clusters to different blocks to provide for wear-leveling, the complexity of the controller hardware and firmware also continued to increase. As manufacturing processes continue to improve and evolve (Micron Technology, Inc., 2008) it is possible that the number of write cycles for each block will increase to the point that wear-leveling will become unneeded or required only in special circumstances. Experimental results have already yielded flash memory that survived 100 million write cycles (Chiu, 2012).

As the cost of NAND flash memory continued to decrease and the density continued to increase, manufactures began to develop total replacement devices for traditional spinning media disk drives for commercial use (Aughton, 2007) and hybrid devices that buffered access to traditional spinning media drives to speed up access to frequently accessed files. Today’s SSD drives that act as a replacement or supplement to spinning media drives are a direct outgrowth of the work done to develop USB flash drives, just in different densities and packaging. Although spinning media drives continue to dominate the marketplace for secondary storage in servers, desktop, and laptop computers with 93% of units shipped in 2012 (Kingsley-Hughes, 2013) an increasing proportion of devices in those settings are being replaced with SSDs as new units are shipped.

One important difference between the USB flash drive and the SSD drives was the difference in expectation about the longevity and robustness of the devices. USB flash drives are most often used as temporary devices that are used intermittently so issues concerning the limited write cycles of the underlying technology (Thatcher et al., 2009, p. 4) are less frequently encountered. As the use of the NAND flash technology was transitioned to use as the primary persistent storage device in desktops and laptops, it was clear that the deliberate spares and wear-leveling that was once a feature to extend the life of a USB flash drive was now a requirement to provide for a reasonable lifespan for the SSD device.

One issue for the manufacture's replacement for spinning media drives with SSD drives was the issue of write time. NOR flash memory is addressable at a byte level (Thatcher et al., 2009) but with a dramatic decrease in memory density (and therefore an increased cost). Because NAND flash memory is only addressable at a block level, entire blocks must be written during a write operation. Write operations to NAND flash memory need a pre-initialized area to successfully perform write operations, so the entire block to be written must be set to a pattern of all binary ones or zeros (Bell and Boddington, 2010, p. 5). This pre-write clear operation adds to the time required for write operations. Manufactures have solved this limitation by pre-clearing unused blocks in the SSD memory area as soon as they become "unused", making pre-initialized blocks available immediately for pending write operations. This decision has two important consequences.

The first consequence of the decision to pre-clear recently released SSD memory blocks was another increase in complexity on the SSD device controller hardware and firmware. With the increased functionality, the device needed to track which blocks were no longer in use and needed to be initialized for subsequent use. The list of blocks to be initialized needed to be acted on by the SSD device as a background task or in a period of inactivity, when not responding to external read or write requests. The controller hardware and firmware also needed to track the list of blocks that have been cleared and made available for use. This list of available blocks was separate from the external view of the SSD drive provided to a connected computer which still saw a file access table structure based on sectors and clusters.

A second, more forensically critical impact of this garbage collection or pre-clearing of blocks in the solid state memory for the SSD device was the erasure through the pre-clear process of any data on the disk other than current allocated files and inactive files that were in a recycle bin awaiting deletion. Deleted from the disk were several types of data that are routinely available to analysts in the examination of spinning media disk drives. Gone are the contents of deleted files, isolated blocks of files that have been partially overwritten, and the slack space left as the difference between the size of a file allocation (to the end of a sector) and the data actually written to a file. Useful information in the slack space of file is no longer possible since each file allocation is within a pre-initialized area of the SSD device. Deleted files immediately have their allocation of blocks released for re-initialization by the controller hardware and firmware of the SSD. Since the operation of the controller hardware and firmware is independent of the operation of the attached computer, the block initialization of released blocks is logically and physically separate of the operation of the attached computer, usually continuing to function whenever power is applied to the SSD drive, whether a computer is attached or not. The implication is that an SSD drive removed from a computer for forensic investigation and powered up in isolation in a lab or workbench would continue the process of clearing the released blocks from deleted files.

Once SSDs achieved a certain level of acceptance, manufactures sought to incorporate the control of the pre-clearing operations into the functioning of the computer’s operating system. Industry organizations for disk drives and their interfaces added to the commands provided through the serial interface to the SSD drives an additional command that alerts the controller electronics in the drive that an area has been deleted and released (Shu and Obr, 2007; T13, 2008). This optional “trim” command (often written all in uppercase as “TRIM”) is in addition to the operation that would be received by the SSD controller electronics to delete a file by removing it from the device’s file allocation table. Since the TRIM command may or may not get sent to the SSD, most SSDs do not rely on that information being provided to mark blocks of semiconductor memory for deletion from the drive. Early versions of the TRIM command were synchronous, requiring the computer sending the command to the SSD to wait for acknowledgement of the command prior to proceeding. Later versions of the specification for the TRIM command allow it to be issued asynchronously and queued (SATA-IO, 2009).

Efforts have also been undertaken by manufacturers of SSDs and other devices using flash memory to standardize flash memory hardware structure and controller interfaces (SNIA, 2014). Although many component producers and device manufacturers see advantages in developing standard hardware and interfaces and view the opportunity to interchange commodity components as a positive development, some large players in the marketplace, notably Samsung and Toshiba (Yinug, 2007) have chosen to not follow suit. Even in cases where standard hardware is in use, manufacturers sill make use of proprietary schemes for wear-leveling, garbage collection, pre-allocation, and data encryption local to the flash memory device.

Solid state drives have no moving arm and no spinning disk to add seek time or rotational latency to the data access time. Read operations on SSD devices averaged 0.01 milliseconds according to Deng (2011). Writing however requires erasing to pre-clear an area to be written. Erase time for the SSD pre-clearing operation are much slower, averaging 2 milliseconds, about

200 times slower that the read operation. It is this difference in read and erase times that pushes most flash memory applications in the direction of pre-clearing deleted and unused block for later use.

Forensic Investigation of SSD Devices

Because forensic programs operate on the attached computer and through the plug compatible connection provided to the SSD drive, most forensic analysis is limited to the tools that usually operate on spinning media drives. The controller hardware and firmware of the SSD drive only expose the blocks of solid state memory that are currently mapped in the SSD to the sectors and clusters known to the attached computer. Blocks that are not currently mapped to exposed sectors and clusters are invisible to attached computer-based forensic software. The forensic software is only able to examine allocated files that would appear to a user in the file system directories, inactive files that still appear in the recycle bin, and transient fragments of files that are scheduled by the SSD device to be initialized. Repeated forensic analysis on an SSD that recently had files deleted would show different results, as the fragments of deleted files were automatically reinitialized by the controller hardware and firmware. In a spinning media environment, repeated forensic analysis of a disk would always produce the same result, as changes to the content of a spinning media disk can only occur when it is written to from the attached computer.

The technology of the SSD devices results in two important impacts on the ability of forensic analysts and investigators to find and understand the data stored on SSD devices. Firstly, in the course of carrying out the wear-leveling function, the contents on any particular file is unlikely to be written in logically sequential blocks, but rather to be scattered across the blocks available on the device, Further, as some blocks fail over time, some of the blocks for a file may be written to the spare blocks that are initially unallocated in production use. The sequencing and addressing of these blocks is under the control of the manufacturer's proprietary algorithms for block allocation. Secondly, as detailed elsewhere, the hardware requirement that blocks be initialized prior to writing and the desire on the part of manufactures to have a ready reserve of initialized blocks ready for writing leads to having blocks of deleted files be re-initialized quickly and cause the contents of data portions of deleted files to remain in the solid-state memory for a very short period of time.

Bell and Boddington (2010) found that within 30 minutes, 99.7% of deleted files had been wiped from the SSD under observation and were not recoverable by standard forensic methods. King and Vidas (2011) looked at a range of devices, files sizes and operating system environments and found far more mixed results. Small files in TRIM-enable environments were removed in times that were consistent with Bell and Boddington's observations. A few large files, especially those in environments where TRIM was not used, remained forensically recoverable in the King and Vidas experiments even after extended periods. The proprietary and undocumented implementation of pre-clearing algorithms, variability in the use of the TRIM command, and differences in the implementation of the flash translation layer all contribute to the differences between devices and the differences between the handling of different types of files.

A less frequent but increasingly present challenge to forensic analysis of SSD devices is encryption of data at the device level (Samsung Electronics, 2009). Computer operating system vendors (Microsoft, 2014a) and third parties (Truecrypt, 2014) have offered whole disk encryption for many years, but SSD manufactures have begun to offer industry standard and proprietary encryption of the data stored in solid state memory. Encryption in the solid state memory further increases the complexity of the controller hardware and firmware and provides another layer of abstraction between the data represented on the solid state memory in data blocks and the cluster or node–based view of the data presented to the connected computer.

Alternative Analysis Methods

One path to follow in the analysis of SSD devices would be to examine the data that exists in allocated files that remain on the device, ignoring deleted files, fragmentary files and information left in slack space. While this path gives up any information that was contained in any deleted file, the method is reliable, does not place saved information the disk at risk and can be carried out with many existing forensic tools. While this approach may seem like giving up and ignoring the challenge of SSD issues, the allocated files in most operating system environments provides many opportunities for forensic analysis including memory swap files, log files, temporary files, and the contents of the registry hives in addition to application data.

Bell and Boddington (2010) show experimentally the differences between deleting a file from a spinning media drive and from an SSD. The file deleted from the spinning media drive remained available for forensics recovery. The file deleted from an SSD was initially available but then disappeared as a result of the garbage collection done on the disk. The authors suggest that SSD drives "… of all types and data stored on such drives should be immediately and henceforth considered to be a 'grey area' as far as forensic recovery and legal validation are concerned…" (p. 12).

Bednar and Katos (2011, p. 4) suggest that the integrated circuit chips of the memory portion of a SSD device be removed and be examined separately from the controller portion of the SSD. Alternatively, the memory could be reinstalled in a SSD with a controller that had been specially prepared to not perform the forensically damaging pre-allocation of deleted blocks. The authors suggest that such actions would be difficult, time consuming, and risky to the remaining data. Such an undertaking would need to be done on an SSD device that had been powered off very shortly after any data of interest had been deleted, since the pre-allocation of deleted blocks happens whenever the disk is idle and powered on, even outside of a computer. Another issue for Bednar & Katos is the presence in some manufacturers SSD controller sets of encryption/decryption capabilities that provide for encryption of the data on the memory chips of the SSD device, independent of any command or software on the attached computer. This encryption could be in place without any action by the computer or the knowledge of its owner.

Gubanov & Afonin's (2012) aptly made reference to Schrödinger's cat to describe the difficulty of knowing whether a file that has been marked for deletion has actually been deleted or not, given the automated nature of the re-initialization of solid state memory. The authors reference the work of Wei, Grupp, Spada, and Swanson (2011) to create custom hardware to read SSD memory chips and then discuss the challenge of developing, testing and supporting such hardware for the limited chance that any data would remain on the chips, given the uncertainty of when blocks of data on the SSD are re-initialized. Gubanov & Afonin also reference the encryption issue, tying it additionally to some manufacturer's implementation of a Secure Erase command that provides the ability to change the SSD's hardware encryption key, rendering all of the data on the semiconductor chips unreadable in a single operation of the SSDs hardware and firmware.

Bonetti, Viglione, Frossi, Maggi, and Zanero (2013) showed a useful framework for evaluating commercial products to indentify and rank the operation of wear-leveling and the re-initialization of released blocks. Their contention and a limited sampling showed there is little uniformity of the implementation of features across different manufactures and models of SSD drives. Nisbet, Lawrence, and Ruff (2013) provided some additional clues based on experimental work to determine how long deleted files would be retained comparing the actions of the TRIM command supported by many operating systems. The TRIM command provides suggestions to SSD devices about file system clusters that have been deleted. The command allows the SSD device to act on that information to mark solid state memory blocks for re-initialization. Their experimental results show that some combinations of file systems and TRIM usage provides for longer “time to live” for blocks available to be re-initialized. Depending on the TRIM-enabled file system in use and the size of the files, within one hour of deletion somewhere between 1% and 100% of the deleted data remains. The metrics provided would be useful to an analyst attempting to decide how to proceed with the examination of a particular commercial product.

A number of commercial services offer the possibility of recovering data from SSD devices in the case of damaged hardware (Ocz, 2014; WeRecoverData, 2014), but none offer the degree of certainty of recovering damaged files as great as for spinning media drives. At least one recovery expert goes so far as to recommend against using SSDs for critical files, relying instead on spinning media (Graham-Smith, 2013). Although widely used for cell phones and other device containing embedded flash memory, chip-off technology, while widely available (Elder, 2012), has been proposed but not widely adopted as a technique for analysis or recovery of data from SSD devices.

Discussion of the Findings

The purpose of this research was to examine the limitations on SSD artifact recovery. Does the technology of SSDs place inherent limitations on the recovery of artifacts of deleted files? What role do the decisions of manufactures and the marketplace play in the difficulty of recovering forensic artifacts? Are there advances in standards or technology that are likely to improve this situation?

Although the operating systems that support SSD devices and the application programs that make use of them do not see SSDs as substantially different from the spinning media drives they are slowly replacing, the differences in the way that data is written onto and erased from SSDs leads to very different results from the perspective of forensic investigations. Because of wear-leveling, the contents of files are scattered across the physical blocks of semiconductor memory in random ways by proprietary algorithms. To provide for the quickest possible write times, deleted and relocated blocks in semiconductor memory are pre-cleared of their content preparing for the next write cycle, obliterating any fragmentary parts or elements of files no longer allocated.

As computing becomes less focused on traditional laptop, desktop, and server environments and continues to spread to pervasive computing (Intille, Larson, Beaudin, Tapia, Kaushik, Nawyn & Mcleish, 2004) and the internet of things (Gershenfelo, Krikorian & Cohen, 2004), persistent storage will increasingly become solid state and spinning media devices will become a legacy environment. As the technology spreads, forensic analysts will increasingly be confronted with SSD environments that do not retain artifacts of deleted files in any predictable way. With a wide variability in the pre-clearing behavior of various operating environments and file sizes, only an examination will determine what deleted file artifacts are available at the time of the examination.

Limitations of the Technology

Although the landscape of file storage is very different for the SSD devices, the tools available to explore it have not changed. Limited as they are to the computer side of the flash translation layer mapping from physical memory to the logical view of the SSD (Kim et al., 2002) as if it were a spinning media device, commercial and open source forensic tools are in most every respect another application program running on a computer that sees the SSD as just another spinning media device. Popular tools like FTK and EnCase capture a forensically sound image of something that looks like a spinning media drive with a file access table, a boot sector, and clusters of allocated and unallocated sectors because that is what the controller hardware and firmware on the SSD tells the program when asked. What the tools cannot see are mapping of semiconductor memory blocks to the virtualization done in the flash translation layer. The tools are also unable to see the blocks that have been marked as damaged and unable to be used. Invisible also is all of the data that has been wiped from the semiconductor memory blocks by the pre-clearing process to prepare blocks of semiconductor memory for reuse and rewriting.

The challenge faced by forensic examiners of SSD devices using conventional forensic tools and techniques goes to the key principal of the stability of digital data under forensic examination. A cornerstone of digital forensics analysis is that the analysis should make no changes to the information under examination unless absolutely necessary. As we now know, any unallocated areas on the disk will continue to be pre-cleared and overwritten as long as power is applied to the SSD. Multiple forensically sound image captures of an SSD to which nothing is being written would be different each time that an image was captured until all unallocated blocks have been initialized for rewriting. Only when nothing other than the allocated files remain on the disk would an image capture be reproducible, a longstanding hallmark of forensically faithful image captures.

The interface of the SSD device to the connected computer allows the use of conventional forensic tools, but the SSD is an intelligent device and the actions of the hardware and firmware cause it to continue to change, even while an image capture is underway. There are not resources available that would render the SSD as a device that is as forensically stable as the spinning media drive. Because of the wide variability in implementation across different drives used in different operating system environments, it is difficult to predict what, if any of the material from unallocated space and deleted files will remain for analysis. Although there exists a desire to improve the ability to recover "lost" data for SSD devices, such recovery seems unlikely.

The technology of SSDs place inherent limitations on the recovery of artifacts of deleted files. The use of NAND memory and the limitation on the number of erase cycles to each block creates the need to scatter write operations cross the memory space available. More critically, the substantially slower erase and write time of NAND memory create a bottleneck that can only be practically solved by tracking available blocks and creating a pool of pre-cleared blocks available for re-use, eliminating forensic artifacts in the process.

Manufacturers and the Marketplace

Any analysis of SSD devices other than through the manufactures' provided interface such as bypassing the controller hardware with chip-off activities or other direct access to the memory chips will be costly, time consuming, and risky to the subject data. Among other considerations, the mapping for the flash translation layer in the controller hardware and firmware, the proprietary nature of the encoding of data on the semiconductor memory, and the possible presence of encryption on the SSD memory under the control of the controller hardware and firmware are all potential challenges in any approach to examination of the data on an SSD drive without the controller. Manufactures have chosen to not implement standards which would provide common interfaces for direct access to the digital memory of SSDs. With SSD drives approaching a terabyte in size, exercises in chip removal and the human resource intensive processes that might be practical for the much smaller memory sizes of a flash memory drive or a cell phone have less usefulness on such a large memory device.

It should be possible to provide a software or hardware “off switch” for the pre-clearing process that a forensic examiner might engage upon arrival at an examination. Such a switch would provide for a forensically stable set of data on the disk and remove much of the uncertainty that surrounds what information is left behind on a disk that is in evidence or at issue. Even if such a facility were mandated, it would only allow the examiner to reliably see the most recently deleted items and prevent the deletion of remaining undeleted artifacts. A pre-clear disable within the SSD would not allow the examiner to see the days, weeks, or months of deleted file fragments that are ordinarily encountered on spinning media drives.

Competition in the marketplace between manufactures prevents the use of standards that would enable forensic examiners to understand the algorithms used for wear-leveling and pre-clearing. Such standards could also provide hardware access to the NAND memory in a standard way in the absence of the controller which would allow the examination of memory without the ongoing risk of pre-clearing operations. The presence of encryption of the memory of the SSD by the controller itself presents a competitive advantage for the manufacturer and difficult challenge for the examiner.

Advances in Standards and Technology

Were it possible to do away with the pre-clearing process and the need to provide for wear-leveling, then the forensic problems with the SSD would disappear and we would be left with a remarkably fast and increasingly affordable disk drive replacement. For spinning media drives with an average read response of approximately 5 milliseconds compared to 0.02

milliseconds for the equivalent operation in an SSD device, this two order of magnitude improvement in performance can make noticeable differences in initial boot time (Jacobi, 2013), the responsiveness of applications, and user perceptions. However, the SSD continues to present the challenges of wear-leveling and pre-clearing behavior, so these issues will continue to be challenges to the forensic examiner.

While there is a requirement that blocks of semiconductor NAND memory be pre-cleared in advance of writing, there is no requirement that they be pre-cleared just after the file is deleted, providing a large pool of memory available for writing. Other alternatives would include pre-clearing some of the blocks and leaving other blocks uninitialized with their forensic load in place for later recovery. Another alternative would be to provide a mechanism to disable pre-clearing altogether, causing the SSD to clear blocks only when a write request had been made. This “just in time” clearing of available blocks would provide for very fast reads and slower writes. Write operations to such an SSD would be slightly faster (at approximately 2 milliseconds) than write operations on current generation spinning media drives (at about 5.5 milliseconds). There seems little possibility that manufacturers would voluntarily provide the capability to cripple or disable the pre-clearing process as there is no performance or competitive advantage in doing so.

Without a technological breakthrough, pre-clearing will continue to be necessary for two reasons. Firstly, the favored NAND memory for the SSD requires that data be written in blocks and that blocks be pre-cleared to all binary ones or zeros. Secondly, the pre-clearing process for NAND memory is substantially slower (2 milliseconds) than the very fast reading times (0.02 milliseconds). Pre-clearing blocks in advance of when they are needed, wiping forensically valuable “garbage” seems the only choice. Improvements in manufacturing techniques could increase the number of write cycles for NAND memory and decrease or eliminate the need for wear-leveling, but spreading writes over the whole area available with wear-leveling is far less of a forensic problem than pre-clearing.

In the absence of technological breakthroughs, analysts should not expect modern systems to retain information about deleted files. If a forensic examination happens to reveal details of recently deleted files in a transient state, then the analyst will need to be able to explain the forensic finding in the context of the ongoing pre-clearing process of SSD devices. Most difficult may be the need to explain how that the contents of the SSD in the initial scan are different that the scan of the SSD that is in evidence or at issue at some later time.

When confronted with the opportunity to look at the contents of NAND memory in the absence of the associated controller, analysts will need specialized tools or customizations for the specific environment. Such chip-off efforts for SSDs will always be less efficient, risky to the data, and more difficult to explain clearly and convincingly when challenged. With flash transition layer mapping and encryption keys in the controller, practical chip-off analysis of SSDs is, at best, problematic.

Although there are advances in the technology of NAND memory that could increase the number of erase cycles to the point that wear-leveling could be substantially reduced or eliminated, there is nothing on the horizon that appears to solve the slow erase time for blocks of NAND memory. It is this physical characteristic of the memory that slows the write cycle and necessitates the pre-clearing of memory to our forensic disadvantage. Nothing short of a breakthrough in technology can reasonably be expected to solve this intractable problem.

The legacy shortcut for spinning media drives that resulted in large amounts of data being left behind when deleting files is being replaced. As SSDs become more popular, the side effect that causes the contents of deleted files to be wiped from storage in un-recoverable ways will be seen more frequently. Although the implementation and execution of these pre-clearing actions are proprietary, undocumented, and vary based on a number of factors, they are clearly integral to the operation of SSDs, a popular and growing segment of the persistent storage marketplace. Forensic examiners will have to learn to deal with this uncertainty in environments under examination.

Recommendations and Future Research

Manufacturers of SSD devices should make available detailed information concerning the rules and algorithms used in the pre-clearing process of deleted files. Research by Nisbet, Lawrence, and Ruff (2013) suggests that not all files are treated the same in the pre-clearing process. Details provided by the manufacturers should include the order in which deleted blocks are processed (size of file, time of deletion, age of file, position in physical memory, or other factors), the speed with which blocks are cleared by an SSD not engaged in other processing, whether the pre-clearing process will continue in the absence of a write-enabled computer, and whether there are actions which would disable the pre-clearing process. Information about the operation of the pre-clearing function would not seem to provide a competitive advantage between manufacturers and the details would be very useful to those studying, examining, and explaining the details of the functioning of a specific individual device.

The use of standard interfaces into SSD controllers from the attached computer and into the solid state memory from the controllers in SSDs as documented in publications from SNIA (2014) would make possible the use of chip-off recovery of data from SSDs in the case of damaged controllers and for forensic recovery without the risk of ongoing pre-clearing operations. There are multiple limitations in such chip-off undertakings, including the flash transition layer mapping for the solid state memory, identification of deliberate spares and damaged blocks, and the possibility of systemic encryption. Even with such limitation and risks, the use of standard interfaces lowers the risk and decrease the cost and engineering expertise necessary to undertake chip-off examination. Manufacturers should make use of standard interfaces for the many reasons outlined in documents from SNIA (2014) and to ease forensic analysis of their systems.

Burnett (2012) suggested that a topic for future research would be a catalog of behaviors related to pre-clearing across various SSD manufactures, models, operating system environments, use of the TRIM command, and file sizes. Nisbet, Lawrence, and Ruff (2013) in the course of their research made a start at such a catalog. Such a catalog would provide an ongoing resource to forensic examiners and analysts concerning what to expect when examining SSDs. A catalog would provide external validation showing why that the forensic examination of an SSD would change over time, as deleted blocks were pre-cleared. Challenges in such a catalog would include the variety of operating system environments, the proliferations of devices, and the volume of data to analyze as SSDs continue to increase in capacity. In early 2014, 96 models of SSD devices from 12 manufacturers were available for use as replacements for spinning media (Microcenter, 2014). They ranged from 32 gigabytes to 1 terabyte in capacity.

One protocol that could be implemented to examine the details of the pre-clearing operations of SSDs in the widely used PC and Windows environments would be one that would limit the storage and time requirements of the analysis by limiting the size of the volume allocation on the SSD. By formatting the SSD drive to some size smaller than the total allocation of the drive, for example limiting the allocation of a larger drive to two gigabytes, would make it possible for the examiner to quickly gather multiple sample image captures of the allocation over the course of a defined period. Using Access Data's FTK Imager (SANS Institute, 2008) or some similar tool to produce forensically sound images, six images of the two gigabyte allocation would fit on a 32 gigabyte flash drive for capture, transport, and analysis with room left over for the toolkit. By using a standard mix of file sizes and then performing the delete in a documented fashion, the examiner could capture and then document the actions of SSDs currently in the marketplace and new ones as they appear.

Another topic for future research would be following up on the opportunity to provide a switch to disable the pre-clearing function on SSDs that could be activated to prevent further automated erasing of forensic artifacts. The switch could be implemented in a number of ways. A magnetic switch could be added to the SSD package that was activated by a magnet placed at a certain location on the outside of the SSD case. The closing of the magnetically activated switch would signal the processor and firmware of the SSD to disable the pre-clearing function. Another approach would be to make use of the Serial Advance Technology Attachment (SATA) interface that provides the connection between the SSD and external computers (APT Technologies, Dell Computer, Intel, Maxtor & Seagate, 2003). The interface could be altered so that a constant high or low voltage on a specific pin of the connection would signal the processor and firmware of the SSD to disable the pre-clearing process. A special "write protect" adapter for SSD drives could provide the specific voltage level on the correct connector pin when the SSD was powered up, disabling the pre-clearing process. The implementation of such a disabling function for the pre-clearing operation of the SSD would prevent the further erasure of forensic artifacts from the disk during examination and would freeze the data on the disk, making it forensically stable for the first and any subsequent forensic examinations.

What does the future hold? Without a breakthrough, the physics of SSDs dictates that required block erases are dramatically slower than other operations, necessitating the pre-clearing of deleted blocks to preserve device throughput. These recommendations and topics for future research would provide valuable tools for the forensic analysis of what will likely become the new standard for persistent data storage. The embarrassment of riches provided by the incomplete erasure of spinning media drives will fade into memory as forensic analysts have to do "…all the running you can do, to keep in the same place" (Carroll, 1871).

References

Adelstein, F. (2006). Live forensics: Diagnosing your system without killing it first. *Communications of the ACM*, 49 (2), p. 63--66.

Antonellis, C. (2008). Solid state disks and computer forensics. *ISSA Journal*, 36--38.

Arpaci-Dusseau, Remzi H., Arpaci-Dusseau, Andrea C. (2014), File System Implementation, Arpaci-Dusseau Books. Retrieved from http://pages.cs.wisc.edu/~remzi/OSTEP/file-implementation.pdf

APT Technologies, Dell Computer, Intel, Maxtor & Seagate (2003). *Serial ATA: High speed Serailized AT attachment*. [online] Retrieved from: http://147.145.44.154/t13/docs2003/e03104r0.pdf [Accessed: 10 Apr 2014].

Aughton, S. (2007). Dell gets flash with SSD option for laptops. [online] Retrieved from: http://www.itpro.co.uk/111350/dell-gets-flash-with-ssd-option-for-laptops [Accessed: 25 Feb 2014].

Ban, A., Moran, D., & Ogdan, O. (2000). *Architecture for a universal serial bus-based PC flash disk*, US Patent 6,148,354. Retrieved from: Google Patent. [Accessed: 12 Feb 2014].

Basic Electronics Tutorials. (2014a). *Logic NAND gate tutorial with logic NAND gate truth table*. [online] Retrieved from: http://www.electronics-tutorials.ws/logic/logic_5.html [Accessed: 10 Mar 2014].

Basic Electronics Tutorials. (2014b). *Logic NOR gate tutorial with logic NOR gate truth table*. [online] Retrieved from: http://www.electronics-tutorials.ws/logic/logic_6.html [Accessed: 10 Mar 2014].

Bednar, P. & Katos, V. (2011). *SSD: New challenges for digital forensics*. [online] Retrieved from http://www.cersi.it/itais2011/pdf/30.pdf [Accessed: 10 Mar 2014].

Bell, G. B. & Boddington, R. (2010). Solid state drives: the beginning of the end for current practice in digital forensic recovery?. *Journal of digital forensics, security and law*, 5 (3), p. 1--20. [online] Retrieved from http://www.jdfsl.org/subscriptions/JDFSL-V5N3-Bell.pdf [Accessed: 20 Mar 2014].

Bonetti, G., Viglione, M., Frossi, A., Maggi, F., & Zanero, S. (2013, December). A comprehensive black-box methodology for testing the forensic characteristics of solid-state drives. In *Proceedings of the 29th Annual Computer Security Applications Conference* (pp. 269-278). ACM.

Burnett, B. (2012). *The effect of the solid state drive on computer forensics*. Master of Science. Utica College.

Carroll, L., 1871. *Through the looking glass*. 1st ed. London: Macmillan.

Chiu, Y. (2012). *Flash Memory Survives 100 Million Cycles*. [online] Retrieved from: http://spectrum.ieee.org/semiconductors/memory/flash-memory-survives-100-million-cycles [Accessed: 20 Mar 2014].

Computer History Museum. (2012, July 17). *Main timeline of significant events and products*. [online] Retrieved from http://chmhdd.wetpaint.com/page/Main Timeline of Significant Events and Products

Cooney, M. (2012, July 5). *DHS looking for forensic tools to lift evidence from solid state drives*. [online] Retrieved from http://www.networkworld.com/community/blog/dhs-looking-forensic-tools-lift-evidence-solid-state-drives

Da Cruz, F. (2001, February). *IBM 2301 drum storage*. [online] Retrieved from http://www.columbia.edu/cu/computinghistory/drum.html

Deng, Y. (2011). What is the future of disk drives, death or rebirth?. *ACM computing surveys,* 43 (3), p. 23.

Ekker, N., Coughlin, T., & Handy, J. (2009). Solid state storage 101: An introduction to solid state storage [White paper]. Retrieved from http://www.snia.org/apps/group_public/ downloa d.php/35796/SSSI%20Wht% 20Paper%20Final.pdf

Elder, B. (2012). Chip-off and JTAG analysis. *Evidence Technology*, 10 (3), p. 10-15. Retrieved from: http://www.evidencemagazine.com/index.php?option=com_content&task=view& id=922

Freitas, R., & Chiu, A. (2010, February). *Solid-state storage: Technology, design and applications*. [online] Retrieved from http://static.usenix.org/event/fast10/tutorials/T2.pdf

Garfinkel, S. (1999). USB deserves more support. *The Boston Globe*, 20th May, p. C4. [online] Retrieved from: http://simson.net/clips/1999/99.Globe.05-20.USB_deserves_more_ support+.shtml

General Precision (1964). *BRL report*. [online] Retrieved from: http://ed-thelen.org/comp-hist/BRL64-l.html#LGP-30 [Accessed: 14 Feb 2014].

Gershenfelo, N., Krikorian, R., & Cohen, D. (2004). The Internet of Things-The principles that run the Internet are now creating a new kind of network of everyday devices. *Scientific American*, 291(4), 46-51.

Graham-Smith, D. (2013). *Avoid SSDs for important files, says data recovery firm*. [online] Retrieved from: http://www.pcpro.co.uk/news/385498/avoid-ssds-for-important-files-says-data-recovery-firm [Accessed: 27 Feb 2014].

Gubanov, Y. & Afonin, O. (2012). *Why SSD drives destroy court evidence and what can be done about it*. [online] Retrieved from: http://forensic.belkasoft.com/en/why-ssd-destroy-court-evidence [Accessed: 18 Jan 2014].

IBM (2014). *IBM archives: IBM 350 disk storage unit*. [online] Retrieved from: http://www-03.ibm.com/ibm/history/exhibits/storage/storage_350.html [Accessed: 22 Feb 2014].

Intille, S., Larson, K., Beaudin, J., Tapia, E., Kaushik, P., Nawyn, J. & Mcleish, T. (2004). *The PlaceLab: A live-in laboratory for pervasive computing research*. [online] Retrieved from: http://alumni.media.mit.edu/~emunguia/pdf/IntilleETAL05.pdf [Accessed: 23 Mar 2014].

Jacobi, J. (2013). *Benchmarks don't lie: SSD upgrades deliver huge performance gains*. [online] Retrieved from: http://www.pcworld.com/article/2048120/benchmarks-dont-lie-ssd-upgrades-deliver-huge-performance-gains.html [Accessed: 27 Mar 2014].

Kaufman, L. (2011). Learn how to securely delete files in windows. [online] Retrieved from: http://www.howtogeek.com/72130/learn-how-to-securely-delete-files-in-windows/ [Accessed: 24 Feb 2014].

Kessler, G. (2014). File signatures. [online] Retrieved from: http://www.garykessler.net/library/file_sigs.html [Accessed: 25 Feb 2014].

Kim, J., Kim, J. M., Noh, S. H., Min, S. L. & Cho, Y. (2002). A space-efficient flash translation layer for compactflash systems. *Consumer Electronics, IEEE Transactions On*, 48 (2), pp. 366--375.

King, C., & Vidas, T. (2011, May 13). *Empirical analysis of solid state disk data retention when used with contemporary operating systems*. [online] Retrieved from http://www.dfrws. org /2011/proceedings/17-349.pdf

Kingsley-Hughes, A. (2013). *SSDs set to grab over one third of PC storage solutions market by 2017*. [online] Retrieved from: http://www.zdnet.com/ssds-set-to-grab-over-a-third-of-the-pc-storage-solutions-market-by-2017-ihs-7000015014/ [Accessed: 18 Jan 2014].

Li, K. & Yang, C. X. (2007). Newest SSD Technology and PC Memory System Structure Improvement Research. *Computer Knowledge and Technology (Academic Exchange)*, 3, 094.

Lsoft Technologies Inc. (2014). *NTFS information: hard disk drive basics*. [online] Retrieved from: http://www.ntfs.com/hard-disk-basics.htm#Sectors%20and%20Clusters [Accessed: 22 Feb 2014].

Masuoka, F. & Iizuka, H. (1985). *Semiconductor memory device and method for manufacturing the same,* US Patent 4531203. Retrieved from: Google Patent.

Mckendrick, D. G. (2001). Global strategy and population-level learning: the case of hard disk drives. *Strategic management journal*, 22 (4), p. 307--334.

Microcenter. (2001). *Micro center e*update email*. [online] Retrieved from: http://web.archive.org/web/20010526124036/http://www.microcenter.com/monthly_specials.html [Accessed: 25 Feb 2014].

Microcenter. (2014). *Solid State Drives (SSD)*. [online] Retrieved from: http://www.microcenter.com/search/search_results.aspx?Ntk=all&N=4294945779&cat=Solid-State-Drives-(SSD)%7c512-%3a-Hard-Drives-%26-Data-Storage-%3a-Computer-Parts-%3a-Micro-Center [Accessed: 5 Apr 2014].

Micron Technology, Inc. (2008). Micron collaborates with Sun Microsystems to extend lifespan of flash-based storage, achieves one million write cycles. [press release] December 17,

2008. Retrieved from: http://investors.micron.com/releasedetail.cfm?ReleaseID=440650 [Accessed: 25 Feb 2014].

Microsoft. (2000). *File Systems and data store changes.* [online] Retrieved from: http://msdn.microsoft.com/en-us/library/ms834188.aspx. [Accessed: 25 Feb 2014].

Microsoft. (2014a). *Bitlocker drive encryption overview*. [online] Retrieved from: http://windows.microsoft.com/en-us/windows-vista/bitlocker-drive-encryption-overview [Accessed: 25 Feb 2014].

Microsoft. (2014b). Recover files from the recycle bin - Microsoft Windows help. [online] Retrieved from: http://windows.microsoft.com/en-us/windows/recover-files-recycle-bin#1TC=windows-7 [Accessed: 25 Feb 2014].

Narayanan, D., Thereska, E., Donnelly, A., Elnikety, S., & Rowstron, A. (2009, April). Migrating server storage to SSDs: analysis of tradeoffs. In *Proceedings of the 4th ACM European conference on Computer systems* (pp. 145-158). ACM.

Newegg. (2014). USB flash drives, UDSB thumb drives. [online] Retrieved from: http://www.newegg.com/USB-Flash-Drives/SubCategory/ID-522?&cm_sp=Flash-Memory324-_-VisNav-_-USBFlashDrive [Accessed: 25 Feb 2014].

Nisbet, A., Lawrence, S. & Ruff, M. (2013). A forensic analysis and comparison of solid state drive data retention with trim enabled file systems. *SRI Security Research Institute, Edith Cowan University, Perth, Western Australia*.

Ocz. (2014). *Ocz SSD data recovery services*. [online] Retrieved from: http://ocz.com/consumer/support/ssd-data-recovery [Accessed: 27 Feb 2014].

Pal, A. & Memon, N. (2009). The evolution of file carving. *Signal processing magazine, IEEE,* 26 (2), p. 59--71.

PCtechguide. (2011). *Hard disk (hard drive) performance - transfer rates, latency and seek times*. [online] Retrieved from: http://www.pctechguide.com/hard-disks/hard-disk-hard-drive-performance-transfer-rates-latency-and-seek-times [Accessed: 24 Feb 2014]

Podlipnig, S. & Schnhart, S. (2014). *Magnetic drum*. [online] Retrieved from: http://cs-exhibitions.uni-klu.ac.at/index.php?id=222 [Accessed: 14 Feb 2014].

Rosenthal, D. S., Rosenthal, D. C., Miller, E. L., Adams, I. F., Storer, M. W., & Zadok, E. (2012). The economics of long-term digital storage. *Memory of the World in the Digital Age*, Vancouver, BC.

Samsung Electronics. (2009). Full disk encryption comes to solid state drives. [press release] April 16, 2009. Retrieved from: http://www.samsung.com/global/business/semiconductor/news-events/press-releases/detail?newsId=4119 [Accessed: 25 Feb 2014].

SANS Institute. (2008). *Forensics 101: Acquiring an Image with FTK Imager*. [online] Retrieved from: http://digital-forensics.sans.org/blog/2009/06/18/forensics-101-acquiring-an-image-with-ftk-imager/ [Accessed: 5 Apr 2014].

SATA-IO. (2009). *The path from 3Gb/s to SATA 6Gb/s: How to migrate current designs to the SATA revision 3.0 specification*. [online] Retrieved from: https://www.sata-io.org/sites/default/files/documents/SATA-6-Gbs-The-Path-from-3gbs-to-6gbs.pdf [Accessed: 12 Mar 2014].

Seebach, P. (2005). Standards and specs: the ins and outs of USB. [online] Retrieved from: http://web.archive.org/web/20100110094907/http://www.ibm.com/developerworks/power/library/pa-spec7.html [Accessed: 25 Feb 2014].

Sheward, M. (2012, January 5). *Rock solid: Will digital forensics crack SSDs?* Retrieved from http://resources.infosecinstitute.com/ssd-forensics/

Shu, F. & Obr, N. (2007). Data set management commands proposal for ata8-acs2. *Management,* 2 p. 1.

SNIA. (2014). *Solid state storage standards explained*. [online] Retrieved from: http://snia.org/forums/sssi/knowledge/standards [Accessed: 10 Mar 2014].

StorageNewsletter. (2014). *StorageNewsletter » 39 million SSDs shipped worldwide in 2012, up 129%* [online] Retrieved from: http://www.storagenewsletter.com/rubriques/market-reportsresearch/ihs-ssd-2012/ [Accessed: 18 Jan 2014].

T13. (2008). *Technical Committee T13 - AT Attachment for TRIM*. [online] Available at: http://t13.org/Documents/MinutesDefault.aspx?keyword=trim [Accessed: 11 Mar 2014].

Thatcher, J., Coughlin, T., Handy, J. & Ekker, N. (April 2009). *NAND Flash Solid State Storage for the Enterprise, An In-depth Look at Reliability*. Solid State Storage Initiative (SSSI) of the Storage Network Industry Association (SNIA). Retrieved from: http://www.snia.org/sites/default/files/SSSI_NAND_Reliability_White_Paper_0.pdf [Accessed: 25 Feb 2014].

Thomas, T. (1998). *Manchester drums*. [online] Retrieved from: http://www.tommythomas.org.uk/Manchester/manchester_drums.html [Accessed: 14 Feb 2014].

Truecrypt. (2014). *Free open-source on-the-fly disk encryption software for windows 7/vista/xp, mac os x and linux*. [online] Retrieved from: http://www.truecrypt.org/ [Accessed: 25 Feb 2014].

Turing, A. M. (1936). On computable numbers, with an application to the entscheidungsproblem. *J. Of Math*, 58 p. 345--363.

Wei, M. Y. C., Grupp, L. M., Spada, F. E. & Swanson, S. (2011). *Reliably erasing data from flash-based solid state drives*. 11 p. 8--8. [online] Retrieved from: https://www.usenix.org/legacy/events/fast11/tech/full_papers/Wei.pdf [Accessed: 25 Feb 2014].

WeRecoverData. (2014). *SSD hard drive data recovery by werecoverdata.com*. [online] Retrieved from: http://www.werecoverdata.com/ssd-hard-drive-data-recovery/ [Accessed: 27 Feb 2014].

White, J. (2011). *Storage subsystem resiliency guide*. NetApp technical reports. [report] NetApp, p. 5.

Yinug, Y. (2007). The rise of the flash memory market: its impact on firm behavior and global semiconductor trade patterns. *Journal of International Commerce \& Economics*, p. 137.