Proceedings of 2016 Universal Technology Management Conference (UTMC), Minnesota, United States of America, 2016

Forensics Analysis of Solid State Drive(SSD)

Digital Forensics

Binaya Raj Joshi
School of Interdisciplinary Informatics
University of Nebraska Omaha
Omaha, NE, USA
bjoshi@unomaha.edu

Rick Hubbard
School of Interdisciplinary Informatics
University of Nebraska Omaha
Omaha, NE, USA
rhubbard@unomaha.edu

ABSTRACT—

The need for advanced computer forensics techniques is because of the results of increasing criminal investigation which involves advanced to sophisticated digital misuse of systems. Digital forensics will always be the advanced field as a profession with the rise of laws that governs legal cases and computer technologies which are becoming more and more ubiquitous. This research paper will provide detailed studies of fundamental techniques used over traditional HDD's and upgraded techniques utilized and required over SDD's to perform the digital forensic investigation. Solid State Drives (SDD) rely on flash memory (in some cases uses SRAM or DRAM), which has overtaken traditional spinning platter hard drives to become the standard for secondary storage in laptop computers. Thus, SSD is now becoming more available to desktop computers, laptops, tablets, smartphones and even in memory sticks, memory cards than before. On the basis of previous papers, research and product information available it refers how SDD relies on flash storage, so it is more reliable and faster than the traditional hard drives. The Flash memory is divided into 2KiB, 4KiB or larger rather than into 512 bytes blocks in traditional hard drives. This paper will also describe how the limited lifespan and show self-corrosion for blocks of memory from unallocated space within modern SSD will generate complications during forensic investigations. The analysis performed to accomplish this project involves testing of allocated and unallocated space within SSD's in laptops with TRIM functionality enabled/disabled while using write blocker to identify the differences and analyzing in a forensic investigation in multiple versions of operating system. The garbage collection of hard drive would contain data that was deleted and marks it as deleted making it recover later but with the modern SDD' self-destroying techniques, those sectors are rewritten with new information at all time. This will make it complicated for forensics investigators to recover necessary evidence to prove crimes in front of the court to prosecute the criminals. This research paper will concentrate on exploring methods that could reduce the impact of all features describe at this moment so as to make forensic investigation easier and feasible for SDD in future.

KEYWORDS: Computer Forensics, Flash memory, Solid State Drive(SSD), TRIM functionality.

1. INTRODUCTION

Solid State Drives (SSD) dependent on flash memory (in some cases uses SRAM or DRAM) have overtaken traditional spinning platter hard drives to become the standard for secondary storage in laptop computers. Nowadays notebook, tablet, and smartphone products arguably wouldn't exist without solid-state or flash memory technology for the hard drives. SSD's are considered to have no moving parts such as spinning disks or movable read/write heads which used to be existing in traditional hard drives or floppy disks. In the traditional magnetic hard drive stack of disks covered in magnetic material stores data in the patterns of 0' and 1' thus having the inability to write in the same location each time [2] [15]. So when data has been deleted, it would be marked as erased but would be available in an unused sector where those deleted files could be recovered at all time. But with the advancement of studies and performances, modern SDD are capable of emptying all sector within the drive at all time making it new thus obscuring to recover deleted files. The TRIM functions perform a deletion of invalid data from the memory of SSD's pages to ensure that the re-write operation can be well performed consistently. The feature known as garbage collection, self-corrosion in SDD's will also permanently erase the deleted files in the background from that sector within few minutes or immediately of the data being removed.

Based upon the information gathered and sorted from various scholars and research papers, it makes known that the corrosion of evidence issue in flash memory and sophisticated use of TRIM mechanism causes the hardening of a forensics investigation. The effectiveness of TRIM mechanisms could have a main difference when enabled for file system while collecting deleted data which usually gets stores even after deletion. Once the self-destruction command using TRIM functionality is enabled for wiping the deleted content in the pages then it becomes impossible to stop even if we installed into a write-blocking imaging device [12]. The Capstone project for Master of Science in Cybersecurity submitted by author Fulton does indicate the modern hard drive as "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." [2]. This will also justify to a certain extend how upcoming flash memory SSD are becoming challenging for forensic analyzes.

A brief description of different feature of SSD's concerning forensics investigation are discussed as below:

1.1. Flash memory:

The nonvolatile memory which deletes data at block level are called flash memory. Data stored in a flash memory must be erased first and fore mostly to be rewritten again into those memories which exist commonly in modern SSD. It is identified that devices using flash memory wipe out data at the block level and rewrite data at the byte level or multiple-byte page level [10] [18].

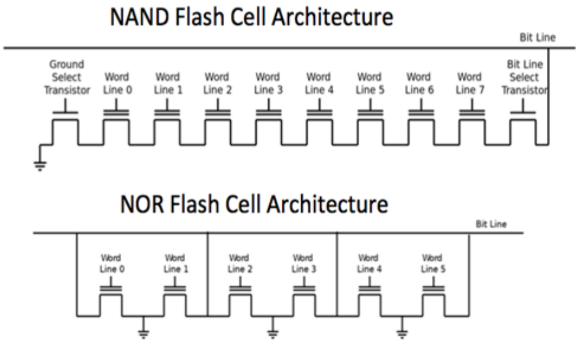


Figure 1: Flash memory architecture [8]

Thus, there are two types of flash memories which are available in the modern SSD's known as NAND and NOR. Table 1 demonstrates a difference in the architecture of NAND and NOR flash memory.

TABLE 1: Differences between NAND and NOR flash memory

NAND	NOR
It is complicated to use.	It is easy to use.
It performs a sequential access on code areas.	It performs a random access on code area
It has higher storage capacity.	It has lower storage capacity.
It performs fast erase than NOR (i.e. fast read and fast write).	It performs slow erase than NAND (i.e. fast read and slow write).
Erase block range from 8Kbytes to 32Kbytes.	Erase block range from 64Kbytes to 128Kbytes.
It is cheaper.	It is expensive.
It rewrites data at the byte level.	It rewrites data at multiple byte levels.

1.2 SLC/MLC/TLC storage:

SLC stands for Single-level cell which is capable of storing bit per cell and two levels of charge. MLC stands for Multilevel cell which are capable of storing multiple bits per cell and multiple levels of charge. TLC stands for a Triple-level cell which are capable of storing three bits per cell and multiple levels of charge.

SLC storage are higher in performance and are faster and much more reliable compare to that of MLC or TLC storage. SLC is also featured with best performing storage arrays while MLC has lower write performance. The most significant use of SLC storage would be to preserve mission-critical applications while MLC could be used for general purposes such as in consumer device or even for general enterprise storage. But TLC is less expensive and have lower performance and durability than SLC and MLC flash memory. TLC is used for sizeable storage such as in USB drives, flash memory cards, smartphones and for other purposes because of its low cost [2] [9]. Figure 2 illustrates the differences between these storages within an NAND flash memory.

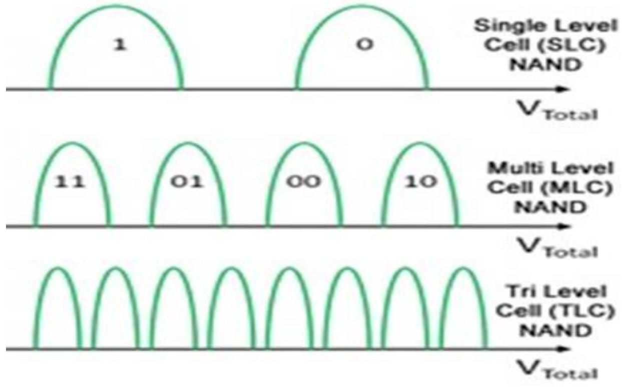

1
0
Single Level Cell (SLC) NAND
V Total
11
01
00
10
Multi Level Cell (MLC) NAND
V Total
Tri Level Cell (TLC) NAND
V Total

Figure 2: Difference between SLC/MLC/TLC [9]

1.3 Partition alignment:

It refers to the physical sector size of a hard drive disk that is utilized by the operating systems. The most significant differences in HDD and SSD would be the partition of sector contained by the hard drive. It is referred in intellectual papers that new HDDs uses 4096 Byte physical sector size which is translated by firmware to 512 Byte sector while the SSD utilizes 8 KB and 16 KB pages similar to that of sectors of HDD [11]. The partition alignment becomes important when we are copying content from a regular or traditional hard drive to SDD because some time clusters from HDD writes to multiple pages of SDD. The partition alignments are also necessary for achieving maximum performance and durability of a hard drive [3] [18].

1.4 Embedded controller:

The embedded controller existing within SSD performs the read and write operation all over the memory chip, which also manages the wear leveling of a hard drive. In general, the controller would be similar to that of RAID where it consumes all multiple chips in parallel to speed the processes. In modern SSD's additional storage are available to embedded controller. The figure 3 shows how the controller is embedded within a SSD.

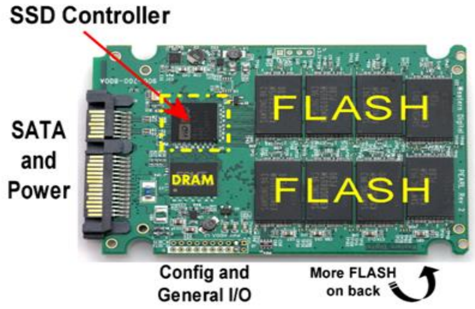


Figure 3: SSD Controller [13]

1.5 Wear leveling:

It refers to a memory management methods developed to extend the lifespan of flash memory [6]. The manufacturer frequently provides extra storage when designing hard drives which are inaccessible by traditional methods could improve the wear leveling a lot better. Usually in SSD's, data are stored in blocks which can be wipe away and rewritten number of times. The wear leveling would handle and ensure that the deletion and rewritten cycles (based upon TRIM command uses) are in an evenly distributed order to perform efficiently and also be able to extend the lifespan of a hard drive. There is two type of wear leveling techniques: Dynamic and Static. Also, manufacturer would have information and techniques on how to access and utilize those extra storages by exchanging with live storage which would improve the wear leveling

1.6 TRIM Functionality:

It is a process in which the flash memory controllers delete the data off the block sector which has been erased by the users and are marked as deleted. It has been referred in an article how SSD's could implement Deterministic Read After TRIM (DRAT) or Deterministic Zeroes After TRIM (DZAT) returning all zeroes immediately after TRIM command executes a certain block of data. But some SSD's will return original data based on the garbage collection algorithm applied inside the designated operating systems. The deletion of data could be performed in the background while users are using the operating systems or can be programmed accordingly as when the machine restarts [6]. "TRIM does not engage in most RAID environments or on external SSD drives attached as USB enclosure or connected via a FireWire port. TRIM does not function in a NAS. Older versions of Windows do not support TRIM. In Windows TRIM is not engaged in file systems other than NTFS. There are specific considerations for encrypted volumes on SSD's, as various crypto containers implement vastly different methods of handling SSD TRIM commands." [12]

1.7 Self-corrosion:

The process in which recoverable elements within hard drives are self-deleted or removed over time that are essentials for performing forensic examinations known as self-corrosion. Regarding modern SSD's, it refers to the process where the controller within flash memory erases the blocks that have been marked as deleted making it complicated for the forensic examiner to recover it [6]. "The evidence self-destruction process is triggered by the TRIM command issued by the operating system to the SSD controller at the time the user deletes a file, formats the disk or deleted a partition. The TRIM operation is completely integrated with partition- and volume-level commands. These includes formatting the disk or deleting partitions; file system commands responsible for truncating and compressing data, and System Restore (Volume Snapshot) operations." [12]. Thus, self-corrosion technique within SSD's for recoverable data that are available these days makes it more challenging towards the forensic investigation.

1.8 Garbage collection:

The NAND flash-based SSD's uses the garbage collection for deleting and rewriting of data into blocks. It states in few research articles that the garbage collection may not necessarily erase all the data immediately that have been deleted by users and marked as invalid by the systems [12] [18]. The garbage collection is not considered as the replacement for the TRIM functionality with SSD's, but TRIM would help the garbage collection be more efficient and improve performance [13]. The garbage collection and the wear leveling are the main reason for the data to be written on the same blocks in SSD's.

1.9 Encryption:

Encryption of hard drives is a process of applying secret key or password to achieve data security to enhance computer hard disks security from intrusion. It safeguards the hard drive by the implementation of protection to each sector which also challenges the forensic investigation. Research studies have shown how solid state hard drives are capable of marking the deleted data as invalid but not necessary erase from the page in the flash memory. Thus, if sensitive data are not well encrypted at all time during the complete process of handling and deletion of data then it may be recovered likewise in the traditional hard drives [2] [10] [13]. Highly skilled peoples could use encryption methods and third party tools such as BitLocker, TrueCrypt, PGP and another standard tool to achieve the highest level of data security in SSD's. These factors would bring more challenges and complications during forensics examination of data analysis of SSD's.

Thus with the rapid growth of computerized crimes, such as invasion, data were stolen, illegal actions, sophisticated hacks into governmental systems, digital forensics analysis, and investigation also needs to advance in every area through the growing technologies. These would involve the cautious collections and examinations of electronic evidence in modern SSD's without damaging the computer and recovering almost all lost information from the system to serve as a strong evidence in the court. This research paper will mainly focus on the SSD within laptops to improve the efficiency of forensics investigation without seeking to replace the extensive resources available. It is necessary for computer security professionals to understand every up-to-date skill required to extract essentials data of modern SSD. A complete imaging of the SSD's hard drive instantaneously could make it possible for forensic examiners to get the image copy with hash value which could serve as evidence in the court during any criminal investigations. Also, manufacturers of hard drive usually design drives with extra storage which is not accessible by the operating system by traditional methods. Thus, research performed and data collected will show how flash memory, controller, TRIM functionality, self-corrosion, wear leveling garbage collection, encryption and other modern features with SSD operates making it tougher for forensic examiner during an investigation. Also, this paper would talk about overprovisioning in SDD's and how manufacturers are complicating the access to the extra storage and also their implementation which are the complication to forensic investigation.

2. RELATED WORK

There exist a large body of research completed for the analysis of solid state hard drives concerning with the forensics investigation for recovering the deleted files in the past. The general steps during evidence collections involves acquisition, authentication, and analysis of hard drives also needs an update with the rising use of SSD's and hybrid drive in modern laptops There have been numerous criminal investigations involving digital examinations of hard drives for evidence to prove crimes in the court to punish the culprit. Many scholarly types of researches and studies have proven toward getting the upmost advancement of the forensics analysis of the regular hard drives. Research studies have led the forensic investigation to require sophisticated carving techniques or mechanisms to acquire essential content of the SSD drives which could help simplify task during forensics examinations [7]. While research studies have shown that TRIM would require the supporting operating systems, specific disk format and cable connections, storage controller configuration to be configured in IDE or ACHI mode and also supporting firmware to perform it tasks [5] [10] [12] [17].

Research studies have shown how deleted file from system on magnetic hard drive just marks it as deleted but can be recovered using forensic techniques. The traces of data which was rewritten on the track of magnetic disk of HDD would basically remain underneath the newer data making it recoverable [8] [11] [15]. But modern SSD mechanism is slightly different than the traditional and could erase all data that were deleted from overwriting in that sector known as pages. [5] [14]. Research studies have also shown how garbage collection in SSD should erase the data contained in pages for the disk to rewrite which can never be recovered by any means [12]. Because of flash memory and controller within SSD's, the performance of the SSD's is also much faster than the magnetic disk HDD's [15] [18]. The previous paper by Marten and Zimmerman have also stated how a calculated hash of an SSD changes as controller overwrites the sectors/pages [6].

There have also been several papers and research studies completed to support SSD data retention with TRIM enabled file systems to ease any digital investigation of hard drives. The past studies have shown how enabling TRIM causes the operating systems to delete file each time so that the sector remains empty at all time to re-write contains in those sectors [3]. While research studies have shown that the disabling the TRIM mechanism in any devices with SSD hard drive would leave less amount of data for forensics analysis making it more complicated for gathering evidence [10].

It is identified through research studies that modern SDD are capable of self-corrosion which makes it difficult to provide strong evident to the court through forensic investigation. The current SSD does have garbage collection which would hold data that are marked as deleted, but can be permanently deleted by overwriting mechanism to have that sector as new at the time [12] [18]. These would make the forensic investigator tough for recovering evidence from an SDD causing the evidence to be tampered during a court case [2].

Overall, these kinds of research studies validate how flash technology in SSDs differ from the traditional HDDs and makes it complex for recovering evidence during a forensic investigation [7] [10]. Previous researchers have also acknowledged how immoral people with advance knowledge level can completely wipe off the hard drive so that the deleted files couldn't be recover under any circumstances later [3] [18]. Also, it has been identified that manufacturers of modern SSD's eliminate away their implementation methods of the hard drives making it difficult for forensics examiners to extract recoverable data from it [12] [18] [19]. The research primarily based on the past study by Marten and Zimmerman (previous student of UNO) has also revealed and concluded that the analysis of forensic challenges posed by flash devices as becoming difficult and almost impossible to capture the actual happening [6]. The paper also exposes how the TRIM mechanisms was more sophisticated in the SSD and problematic while trying to capture changes and hash to maintain the chain of evidence during a forensics investigation [6]. This research project illustrates how modern techniques such as TRIM functionality capabilities, self-corrosion occurrence which are implemented in the SSD would cause complications with a forensics investigation.

3. PURPOSES

This research performed will provide detail analysis and study of results as listed below:

i. Primarily, our research paper will explain the use and live response towards enabling/disabling of TRIM functionality, garbage collection, self-corrosion.
ii. We will list steps to identify whether a hard drive is traditional HDD or SSD or modern hybrid to enhance the performance of analysis.
iii. We will also present recommendations to overcome the challenges with TRIM on modern SSD's forensics.
iv. The paper will focus only on the SSD's available on laptops for enhancement towards forensics investigation and also determine it the SSD is self-corrosive or not.
v. Distinguish the difference between traditional HDD with SSD's with regards to forensics investigation.
vi. Explain the use of write blocker on both traditional HDD and SSD's to extract as much data as possible before complete deletion occur.

vii. Provide detail investigation for challenges of SSD forensics with respects to its firmware, embedded controller, multiple storage and other factors.

viii. Describe the effect of encryption on traditional HDD analysis and SSD for future references.

4. SOLID STATE DRIVE VS. TRADITIONAL HARD DRIVE

The traditional hard drive would work on a magnetic disk platter where the platters are coated both sides so as to store data in a magnetic form. Thus, all data are stored on both upper and lower surface of the platters as tracks which is further divided into individual sectors. So when an operating machine is power on the disk comes in use, and the OS needs to be able to read the correct sector by spinning as fast as it can.

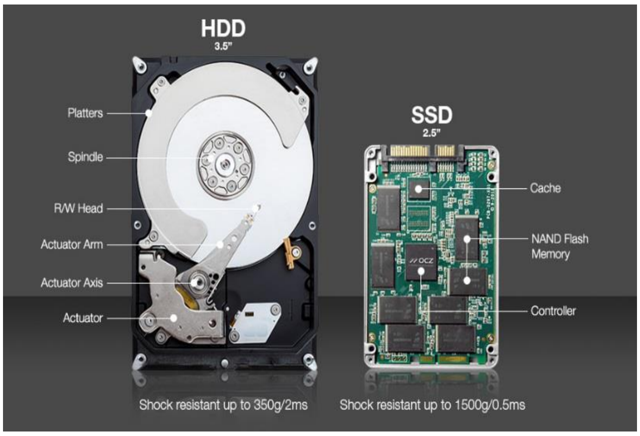


Figure 4: Magnetic Disk vs. Flash memory [16]

While in the case of modern solid state hard drive, it works on flash memory which would not require any moving parts or spinning platter like in traditional hard drives. These have resolved the problems which were arising from the mechanical spinning plates while reading in the disk of HDD. The key components of an SSD are significantly the controller and the memory to store the data.

Figure 5 shows a detail view of SSD device architecture and how modern SDD would have its feature such as flash memory, garbage collector, wear leveling, controller known as block manager are separate and not compact under the same magnetic disk like in traditional HDD.

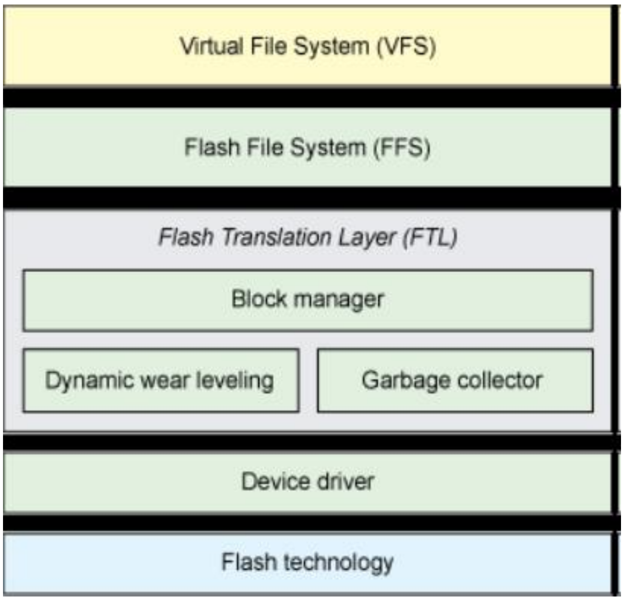


Figure 5: SSD device architecture [16]

5. FORENSICS FOR TRADITIONAL HARD DRIVES

The main purpose of a forensics investigation is to apply extensive procedures and methods that could recover deleted files to prosecute criminals in the court. Since the amount of data that needs to be analyzed, examined and processed could be vast, and the variety of data types could be enormous, forensic investigation team always need to stay ahead of the game. The forensics examination of hard drives by FBI or other examiners has been followed strictly based upon performing the acquisition, authentication and analysis followed by a chain of custody with complete documentation in place, which is considered as a standard [12] [18]. The traditional way of obtaining evidence from a HDD would involve imaging of dedicated hard drive followed by detail analysis with standard evidence discovery tool.

6. PERFORMED EXPERIMENTS AND RESULTS

Before proceeding forward with our memory analysis, we determined if it’s a HDD or SSD or a hybrid drive before running forensic investigation command. Different factors such as the type of operating system, disk formats and cable connected to SSD could affect the TRIM functionality. This section provides a detail information’s regarding several experiments and steps to perform those tests and the results generated through those experiments.

Below tables show the trim functions supported/not supported operating systems, disk format, and cable format accordingly:

TABLE 2: Different operating system supporting TRIM

Operating Systems	**Trim functions**	**Date Introduced**
Windows 7 and newer	supported	October 2009
Windows Vista and older	-does not support and not issued -possible through third party solutions	
Mac OS X 10.6.8 and newer	supported	23 June 2011
Mac OS older than 10.6.8	-does not support + user's installed SSD's excluded from TRIM support	
Linux kernel 2.6.28 and newer	supported	25 December 2008
Android	supported	24 July 2013

TABLE 3: Different Disk Format supporting TRIM

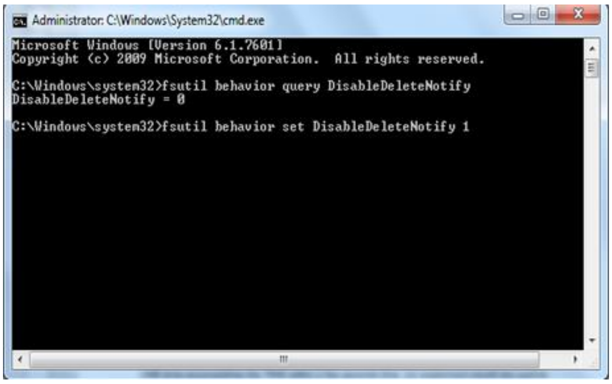
Disk Format	**Trim functions**
NTFS	supported
FAT, FAT 32, ex-FAT 32	not supported
VFAT	supported by mount option 'discard' not manually with fstrim
ext4	supported
ext3, ext2	not supported
HFS+	supported
HFS	not supported

TABLE 4: Different cable connections to hard drives supporting TRIM

Cable Format	**Trim functions**
SATA, eSATA	supported internally but not using USB connector
Firewire	not supported
USB drives or USB (1.0-3.0) connected SSD's	not supported
NAS	not supported
RAID	not supported

Experiments with steps to perform the test again consist two stages performed over the Windows machine with TRIM functionality as described below:

Below figures show how you would enable and disable TRIM in Windows 7 machine

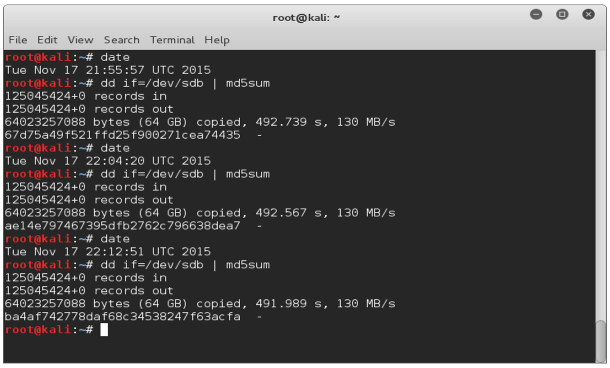


```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Windows\system32>fsutil behavior query DisableDeleteNotify
DisableDeleteNotify = 0

C:\Windows\system32>fsutil behavior set DisableDeleteNotify 1
```

Figure 6: Enabling/Disabling TRIM in windows 7 machine

Stage 1:

1. Load fresh install of Windows 7 Professional SP1 on SVP200S3/60G SSD.
2. Copy files with keywords to SSD.
3. Delete files and immediately shut down the computer.
4. Copy SSD to a hard drive in duplicator (optional).
    a. Compare hashes of SSD and hard drive.
5. Connect SSD to write blocker and generate the hash.
6. Use file recovery utility to search for keywords.
7. If successful, wait 1 hour, take the hash and compare, try the search again.



```
root@kali:~# date
Tue Nov 17 21:55:57 UTC 2015
root@kali:~# dd if=/dev/sdb | md5sum
125045424+0 records in
125045424+0 records out
64023257088 bytes (64 GB) copied, 492.739 s, 130 MB/s
67d75a49f521ffd25f900271cea74435  -
root@kali:~# date
Tue Nov 17 22:04:20 UTC 2015
root@kali:~# dd if=/dev/sdb | md5sum
125045424+0 records in
125045424+0 records out
64023257088 bytes (64 GB) copied, 492.567 s, 130 MB/s
ae14e797467395dfb2762c796638dea7  -
root@kali:~# date
Tue Nov 17 22:12:51 UTC 2015
root@kali:~# dd if=/dev/sdb | md5sum
125045424+0 records in
125045424+0 records out
64023257088 bytes (64 GB) copied, 491.989 s, 130 MB/s
ba4af742778daf68c34538247f63acfa  -
root@kali:~# 
```

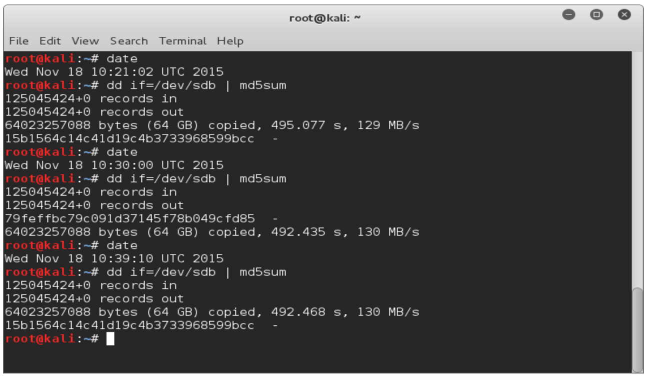
Figure 7: Enabling TRIM in windows 7 machine and getting hash

In the stage 1, we can expect the TRIM functions to make the files unrecoverable. The figure 6 on the right shows the output screen.

Similarly, stage 2 involves disabling TRIM to make the files recoverable

Stage 2:

1. Load fresh install of Windows 7 Professional SP1 to SVP200S3/60G SSD.
2. Copy files with keywords to SSD.
3. Disable TRIM
    a. fsutil behavior set disabledeletenotify 1
4. Delete files and immediately shut down computer
5. Copy SSD to a hard drive in duplicator (optional).
    a. Compare hashes of SSD and hard drive.
6. Connect SSD to write blocker and generate hash.
7. Use file recovery utility to search for keywords.
8. If successful, wait 1 hour, take the hash and compare, try the search again.



```
root@kali:~# date
Wed Nov 18 10:21:02 UTC 2015
root@kali:~# dd if=/dev/sdb | md5sum
125045424+0 records in
125045424+0 records out
64023257088 bytes (64 GB) copied, 495.077 s, 129 MB/s
15b1564c14c41d19c4b3733968599bcc  -
root@kali:~# date
Wed Nov 18 10:30:00 UTC 2015
root@kali:~# dd if=/dev/sdb | md5sum
125045424+0 records in
125045424+0 records out
79feffbc79c091d37145f78b049cfd85  -
64023257088 bytes (64 GB) copied, 492.435 s, 130 MB/s
root@kali:~# date
Wed Nov 18 10:39:10 UTC 2015
root@kali:~# dd if=/dev/sdb | md5sum
125045424+0 records in
125045424+0 records out
64023257088 bytes (64 GB) copied, 492.468 s, 130 MB/s
15b1564c14c41d19c4b3733968599bcc  -
root@kali:~# 
```

Figure 8: Disabling TRIM in windows 7 machine and getting hash

In this stage 2, we can expect the TRIM-disabled state to make files recoverable.

6.1 Result and Findings

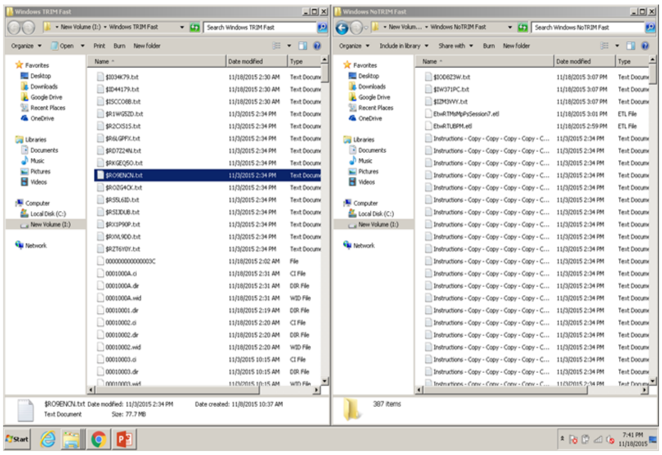


Figure 9: Recuva comparison of Files recovered after TRIM functionality in Windows

We had deleted 384 files and shut the machine to report the hashes. We found that all deleted 378 files were still fully recovered using Recuva when TRIM was enabled. It was available in thousands of file fragments in which 369 were the original files, 12 files were renamed by intact($Rglfdg845) and 3 out of the 384 files renamed with original filename content.

But when we disabled the TRIM repeated the same process in Windows machine, we were able to get the same 378 files out of which 381 were the original files, 0 were renamed but intact and three files were renamed with original file name content.

The below experiments also include using a Linux system (kernel 2.6.33 or newer) to test the TRIM enable and disable functionality described as below:

Stage 3:

1. Load fresh install of Linux version 2.6.28 to SVP200S3/60G SSD
2. Determine if TRIM is supported or not using command below:
    a. sudo hdparm -I /dev/sda | grep "TRIM supported"
    b. An output with message "Data Set Management TRIM supported (limit 8 blocks)" must be displayed else your SSD doesn't support TRIM.
3. To determine if primary storage is SSD
    cat /sys/block/sda/queue/rotational

Results: 0->SSD 1->HDD

4. To determine if continuous TRIM is enabled

-i discard /etc/fstab

If primary partitions have "discard" option, continuous TRIM is enabled

5. To check for scheduled TRIM

sudo grep -ri fstrim /etc

Will show any usages of fstrim command in cron configurations

6. To determine if discard option will enable continuous TRIM

cat /sys/block/sda/queue/discard_zeroes_data

#Results: 0->TRIM will not function 1->TRIM will function

7. To determine if TRIM is detected by operating system

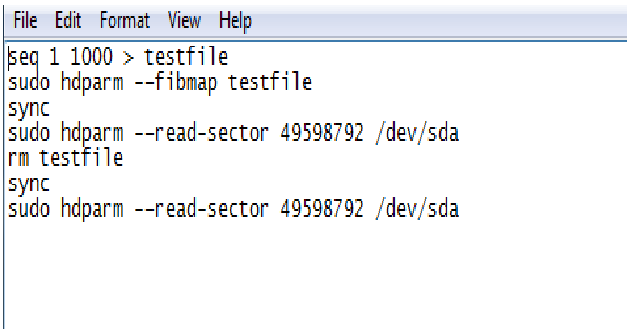
hdparm -I /dev/sda | grep TRIM

Results if detected

* Data Set Management TRIM supported (limit 1 block)

8. If DRAT or DZAT is detected
9. To disable all cron jobs

/etc/init.d/crond stop



```
seq 1 1000 > testfile
sudo hdparm --fibmap testfile
sync
sudo hdparm --read-sector 49598792 /dev/sda
rm testfile
sync
sudo hdparm --read-sector 49598792 /dev/sda
```

Figure 10: Output screen from Linux system

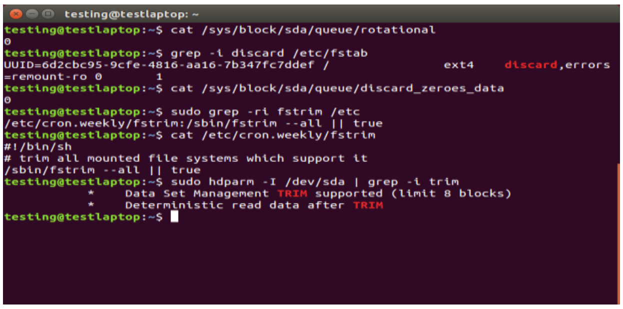
Stage 4:

Create disc image of Ubuntu 15.10 and 14.04.3 version and verify the steps below:

1. Load fresh install of Ubuntu and SVP200S3/60G SSD
2. Determine each version of Ubuntu before proceeding as follow

Ubunto 14.10 and onwards

$ tail –n1 /etc/cron.weekly/fstrim
/sbin/fsrim –all || true



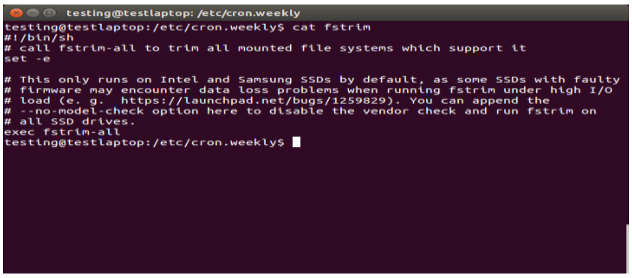
```
testing@testlaptop:~$ cat /sys/block/sda/queue/rotational
0
testing@testlaptop:~$ grep -i discard /etc/fstab
UUID=6d2cbc95-9cfe-4816-aa16-7b347fc7ddef /               ext4    discard,errors
=remount-ro 0       1
testing@testlaptop:~$ cat /sys/block/sda/queue/discard_zeroes_data
0
testing@testlaptop:~$ sudo grep -ri fstrim /etc
/etc/cron.weekly/fstrim:/sbin/fstrim --all || true
testing@testlaptop:~$ cat /etc/cron.weekly/fstrim
#!/bin/sh
# trim all mounted file systems which support it
/sbin/fstrim --all || true
testing@testlaptop:~$ sudo hdparm -I /dev/sda | grep -i trim
           *    Data Set Management TRIM supported (limit 8 blocks)
           *    Deterministic read data after TRIM
testing@testlaptop:~$ 
```

Figure 11: hdparm 15.10 & fstrim in cron.weekly 15.10

Ubuntu 14.04

Scheduled TRIM is enabled by default for Intel, SAMSUNG, OCZ, Patriot and SanDisk SSDs. You could disable the vendor check by running the command:

sed –I ‘s/exec fstrim-all/exec fstrim-all –no model-check/g’ /etc/cron.weekly/fstrim



```
testing@testlaptop:/etc/cron.weekly$ cat fstrim
#!/bin/sh
# call fstrim-all to trim all mounted file systems which support it
set -e

# This only runs on Intel and Samsung SSDs by default, as some SSDs with faulty
# firmware may encounter data loss problems when running fstrim under high I/O
# load (e. g.  https://launchpad.net/bugs/1259829). You can append the
# --no-model-check option here to disable the vendor check and run fstrim on
# all SSD drives.
exec fstrim-all
testing@testlaptop:/etc/cron.weekly$ 
```

Figure 12: hdparm 14.04.3 & fstrim in cron.weekly 14.04.3

Ubuntu 13.10 and Earlier

There are three ways to perform TRIM

i. Manual

sudo fstrim /

For Ubuntu 14.0 and earlier fstrim is not available so you must use below command:

/usr/share/doc/hdparm/contrib/wiper.sh.gz

ii. Scheduled

This process is recommended

iii. Automatic

This is a slow and deprecated process

7. CHALLENGES OF SSD FORENSICS AND SOLUTIONS

The implementation of NAND flash memory with pages to store and reuse blocks in SSD's would make it different in applying forensics techniques and methodologies compared to that of a traditional hard drive. Moreover, complicated encryption methods and sophisticated third party tools are making it tougher to obtain complete memory analysis from a regular hard drive nowadays. Thus, IDE would allow the forensic examiner to perform logical data reads of SSD to acquire data but also can hide internal data structures which could complicate the investigation. Also some manufacturers of SSD's make it complicate or almost impossible to retrieve data reads to protect their implementation details thus making it tougher for forensics examiners [1]. With the growing use of SSD with newer operating systems which would support and enable TRIM by default allow the deleted data to be completely erased making it a dead end to examiners. From our research, we also found that the TRIM and garbage collection are not the same thing in SSD rather TRIM functions help perform garbage collection in a uniform order. The garbage collection would move all the invalid data during the garbage collection process while the TRIM command is sent directly through the operating system to the SSD to identify the invalid data and the sector which can be rewritten to improve the performance of the hard drives.

The manufacturer also would have to implement a way to disable self-corrosion by default so that non-techy criminals could be prosecuted for evidence being store and retrieved by the police. Also, the overprovisioning provided by the manufacturer must be in aa efficient manner so that forensic examiners able to retrieve the implementation and storage access when needed during a criminal investigation.

8. SUMMARY AND CONCLUSION

The improvement of the hard drive from old-fashioned to most recent SSD have increased drastically that the methods applied to preserve, identify and extract recoverable deleted files from modern hard drives are almost impossible or none to today's date. In this paper, we conducted the evaluation of TRIM functionality usage over multiple different operating systems, disk formats, and cable format to identify the challenges toward forensic investigation of modern SSD's.

We identified ways to determine whether a hard drive is traditional or modern SSD. Then we looked at multiple operating systems which supports and does not support TRIM function by default or manually using different versions of SSD's. The experiments performed and results show how enabling/disabling TRIM will help improve and reduce the write performance in SSD's and modern operating system. The use of TRIM allows an operating system to inform a SSD regarding blocks of data which are invalid or marked as deleted to wipe out completely internally so that no traces can be recovered. The hash value of a SSD's could vary depending upon when an image was created for analysis and examination purposes.

It has been learned from our studies that modern SSD's would be all right without TRIM functions enable as long as the controller performs a complete delete and rewrite to the pages working as similar to self-corrosion or garbage collection.

9. FUTURE WORK

With growing SSD's with different sophisticated features for complete wipe out functionality capabilities, we recognized that modern SSD's are projected to be getting more and more complicated for future forensic investigation. We examined how feature such as controller, garbage collection, TRIM functionality, wear leveling encryption makes bad guys easy to set free due to lack of digital evidence.

We have also introduced SLC/MLC/TLC in SSD's drive which could also be another factor to perform detail studies to identify efficient ways of performing forensic investigation. Moreover, getting detailed implementation from all SSD's manufactures along with upmost encryption/decryption.

We took an important first step in suggesting a path to practical TRIM functions enable/disable methods for multiple operating systems along with multiple disk formats. Our results indicated that newer operating systems with SSD does enable the TRIM by default but going forward hybrid drives are starting to be in use which require new methods for forensic investigation. The future of hard drive would definitely implement hybrid drives which is a combination of magnetic disk along with flash memory storage which would create more challenges to forensic investigation. So moving forward if detail research on hybrid drives were to be done based upon researches of HDD and SDD than it would

We have just explained the encryption methodologies which are being applied over modern SSD's to secure more thus making it difficult for forensic examiners. Going beyond some recognized encryption/decryption methods & tools, it is worthwhile to conduct detail data analysis of hardware encryption methods used by manufacturing companies which tries to protect it design implementation by complicating to recoverable any data. On SSD if we implement Truecrypt than it may reveal information regarding sector/pages which has valid data on it making the forensic investigation more convenient.

ACKNOWLEDGMENT

The authors would like to thank all reviewers for their helpful comments to improve this paper.

REFERENCES

[1] "Anatomy of Linux Flash File Systems." Anatomy of Linux Flash File Systems. IBM DeveloperWorks. Web. 8. Oct. 2015.

[2] Fulton, John William "Solid State Disk Forensics: Is there a Path Forward?" Utica College, May 2014. Web. 9 Oct 2015.

[3] Gubanov, Yuri, and Oleg Afonin "Why SSD Drive Destroy Court Evidence and What can Be Done About it." Belkasoft: Evidence Search and Analysis Software for Digital Forensic Investigations. Belkasoft, 1 Oct. 2012.

[4] Lee, Eungyu, Joonwoo Lee, Hyeongseok Kang, Kanghee Kim, Sung-Ryul Kim, and Sung Y. Shin "An Implementation Study of a Ghost Drive: Hidden File Store in a Filesystem". (2012): 1796 – 1798. ACM Web. 18 Oct. 2015.

[5] Mao, Chau-yuan "SDD TRIM Operations: Evaluation and Analysis" Site. Natinal Chiao Tung University, July 2013. Web. 9 Oct 2015.

[6] Martin, Nick, and Jeff Zimmerman. "Analysis of the forensic challenges posed by flash devices." University of Nebraska, 15 Nov. 2012. Print. 15 Oct. 2015.

[7] Memon Nasir "Challenges of SSD Forensic analysis". Polytechnic Institute of NYU. Web 16. Oct. 2015.

[8] Miller, Warren. "Understanding the Differences Between NAND Flash and NOR Flash Memory and Key Future Trends. "Avnet. Web. 18 Oct. 2015.

[9] "NAND Flash Data Storage Overview – SLC, MLC and TLC. "Embedded Computing Design. Cactus Technologies Limited. Web. 7 Oct. 2015.

[10] Nisbet, Alastair, Scott Lawrence, and Matthew Ruff "A Forensic Analysis And Comparison of Solid State Drive Data Retention With Trim Enabled File Systems" Site. Edith Cowan University, 4 Dec. 2013. Web.

[11] "Partition Alignment of Intel SSDs for Achieving Maximum Performance and Endurance." Intel, Intel, 1Feb. 2014. Web. 20 Oct. 2015.

[12] "Recovering Evidence from SSD Drive in 2014: Understanding TRIM, Garbage Collection and Exclusions." Forensic Focus Articles. Belkasoft, 23 Sept. 2014. Web.

[13] Rent, Thomas M. "SSD Controller." SSD Controller. Storage Review, 9 Apr. 2010. Web.

[14] Rouse, Margaret. "What is Flash Memory?" SearchStorage. Web. 12 Oct. 2015.

[15] "SSD vs HDD: Difference. Advantages. What to Choose for Hosting a Website?" Web Hosting Reviews Discount Coupons RSS. 21 Aug. 2015. Web.

[16] "SSD vs HDD – Why Solid State Drive." SSD vs HDD. A Toshiba Group Company. Web. 19 Oct. 2015.

[17] "TRIM (ATAB ACS2 Data Set Management Trim Attribute)." The Corsair User Forums RSS. Web. 25 Oct. 2015.

[18] Wei, Michael, Laura Grupp, Steven Swanson. "Reliably Erasing Data from Flash-Based Solid State Drives." University of California, San Diego. Web. 18 Oct. 2015.

[19] Zaddach, Jonas, Anil Kurmus, Davide Balzarotti, Erik-Oliver Blass, Aurelien Francillon, Travis Goodspeed, Moitrayee Gupta, and Ioannis Koltsidas. "Implementation and Implications of a Steath Hard-Drive Backdoor." Proceedings of the 29th Annual Computer Security Applications Conference on ACSAC' 13 (2013): 279 – 288. Print.