IJCSN - International Journal of Computer Science and Network, Volume 9, Issue 3, June 2020
ISSN (Online) : 2277-5420
www.IJCSN.org
Impact Factor: 1.5

Intrinsic Forensic Obscurity of Solid-State Drives and Impact on Digital Evidence Recovery

[1] Song Shombot Emmanuel; [2] Ameer Al-Nemrat; [3] Shehu Mohammed Ahmed

[1] Department of Computer Science, Federal University Lafia
Lafia, Nasarawa State, Nigeria

School of Architecture, Computing and Engineering, University of East London
4 – 6 University Way, E16 2RD, United Kingdom

[2] Department of Computer Science, Federal University Lafia
Lafia, Nasarawa State, Nigeria

Abstract - This research explores the challenges posed by solid state drives (SSD) n digital forensics. Evidence acquisition has never been this stochastic with hard disk drives (HDD) because, they have been the most dominant storage devices since the 1950s. This is why most of the legal and technical guidelines for conducting acceptable forensics are built around hard disk drives. Today, the proliferation of solid state drives in the market has caused unforeseeable turbulence with substantial impact on the way non volatile memory forensics are conducted. This research thoroughly investigates solid state drives architecture through literature review and practical usability, to understand its functionality so that the opportunity for learning can be identified, and a solution can be proposed to bridge the knowledge gap in forensic practice. Series of experiments were conducted and results indicates that solid state drives are structurally different from hard disk drives thus, established forensic guidelines cannot be fully adoptable when dealing with solid state drives.

Keywords – *Digital Forensics, Solid State Drives, Hard Disk Drives, Wear Leveling, Garbage Collection.*

1. Introduction

Digital forensics also referred to as Computer forensics is the systematic procedure of collecting and analyzing digital information which can potentially be used as evidence in Civil, Criminal, or administrative cases (Nelson et al., 2016). Experts have come up with a well defined methodology for conducting forensic Investigation which is made up of evidence identification, collection, preservation, analysis and reporting (Cassey, 2011). Any distortion at any stage of the methodology can frustrate the forensic process and render the evidence inadmissible in legal proceedings (Sibiya et al 2012).

The forensic guidelines widely use in the world today are tailored unambiguously for HDDs. Their architecture permits data to be stored inside tiny concentric tracks on the disk surface. Each track is divided into sectors, and a map of the tracks and sectors on the printed socket board tells the head exactly where to read or write data. When a file is deleted, the operating system only de-allocates the master file table reference that points to the pieces that makes up the file puzzle and registers the space that it uses to take up as empty. This in simple terms means that, when a file gets deleted, only the mapping pointer gets removed and not the actual file whilst the operating system gets the permission to write new files to that location. Until that very location is over-written, the deleted file will reside indefinitely on the hard disk. This in effect provides the window of opportunity for experts to use hardware such as write blockers and specialized forensic tools to carry out digital evidence analysis.

In contrast, Solid State Drives are storage devices which is made by solid state electronic memory chip array (Smith, 2005). It consists of control unit and storage unit (FLASH chip and DRAM chip). The peculiarity of SSD as a primary storage device is the fact that it uses integrated circuit assemblies as memory to store data persistently. Furthermore, (Micheloni, Marelli, and Eshghi, 2012), also gave their own definition of solid state drives as a storage device that incorporates solid state memory and emulates a hard disk drive to store data.

Architectural variation between HDD and SSD is primarily the reason behind the forensic guidelines inefficiencies when working with the later. SSDs posses a dedicated processor for lifespan optimization and they also have uniform latency across the drive as opposed to read/write heads that are constantly in motion over magnetic platters to measure voltage spikes that are spread randomly on the platters. The uniform latency accounts for the speed when accessing data residing on SSDs. Furthermore, SSDs groups memory cells into segments referred to as blocks. These blocks are arranged in rectangular grids with variant sizes depending on the manufacturer of the SSD but typically, 256 kilobytes (KBs) is the most widely used by manufacturers. These blocks are further subdivided into pages of 2-4 KB. A Page is the smallest permissible unit for all read and write operations. However, it is interesting to mention that the smallest erasable unit for all delete operations is an entire block. This delete operation certainly has a serious impact which runs deep to affect forensics procedures (Shey et al., 2016).

Electron tunneling or hot electron injection or insertion is the process used to store electrical charge into the isolated oxide layer. The existence of electric charge in the isolated region creates an electric field. Depending on the presence or absence of an electric field, a machine logical state of 1 and 0 is defined. 1 represents an empty cell, while 0 represents a cell with data in it which is in complete contrast to the traditional disk drive. A high voltage differential is what is needed on the SSD transistors in order to force a charge pass through or out of the floating gate. The process of hot electron injection is the method used to stare charge (Write) into the isolated region and it is also the same process used to remove charge from the isolated region (delete).

However, it is worthy to emphasize that the read operation from the floating gate transistor does not require the high voltage differential to execute just like the write and delete operation.

According to (Bonetti et al., 2014), he mentioned that with time, a gradual degradation of the oxidation layer used in isolating the gate is unavoidable due to the high voltage differential of the read and write operation. The implication of the degradation is, it will only take about (~10,000 – 100,000) write and delete cycles for the memory cell in a solid state drive to lose its non-volatile capability of retaining data. In order for SSD manufacturers to prevent that, they maneuvered their way through efficient write/delete algorithms to improve efficiency and increase the life expectancy of the memory cells.

The SSD controller provides distinct services of wear leveling, bad block mapping, background garbage collection, encryption, read and write caching, read scrubbing and read disturb management. This research tries to understand all the qualities of SSDs and propose an approach that will best be suited for the most efficient method of digital evidence recovery.

2. Materials and Methods

Series of experiments are carried out to understand and evaluate the responsiveness of SSDs in the light of already established non volatile memory forensics guidelines. The results of the experiment will establish the facts and provide suggestions that will shape a sustainable paradigm for carrying out effective SSD forensics. The four experiments conducted are Recovery of Deleted Files, Hash Value Comparison, The Impact of Trim Function on Evidence Recovery and Recovery after formatting SSD.

In setting up the experiment, there are a number of hardware, software and expert toolkits needed to achieve it. Two operating systems were used for the entirety of the experiment and their specification is captured in Table 1. A total of 4 storage Media were used and two expert toolkits were used and their specification is captured in Table 2 and 3 respectively.

Table 1: Operating Systems Specification

Product	***Dell***	***Apple MacBook Pro***
Operating System	Windows 7 Enterprise 64-bit OS	OS X El Capitan 10.11.3
Processor	3.6GHz Intel Core i7	2.6GHz Intel Core i5
Memory	32 GB	8 GB 1600 MHz DDR3
Startup Disk	Standard Disk Drives	Macintosh HD
Graphics	Intel HD Graphics 4600	Intel Iris 1636 MB
Serial Number	55041-029-0127092-86587	C02N7UXRG3QH

Table 2: Storage Media Specification

Product	***Maxtor HDD***	***Apple SSD***	***Samsung SSD***	***Maplin SSD***
Model	Diamond Max Plus 9	SD0128F	960 Evo – SSD-MZ-V6E250BW	USB Disk 3.0 USB Device
Capacity	80GB	128GB	250GB	256GB
Controller	Apple	Apple	Polaris	Maplin
Physical Interconnect	ATA	PCI	PCI Express	USB 3.0
Trim Support	-	Yes	Yes	Yes
Serial Number	Y259MkYE	1431BT41124	8806088540139	001882227

Table 3: Expert Software Specification

Application Name	*FTK Imager Lite Version*	*Access Data FTK Imager*
Manufacturer	Access Data Group	Access Data Group
Version	3.1.1	3.4.2.2
OS Compatibility	Mac OS X Operating System	Windows Operating System

2.1 Experiment 1: Recovery of Deleted Files

***Purpose of Experiment*:** The purpose of this experiment is to investigate the behavior of SSD and HDD in terms of how they operate, if a forensic investigator makes a deliberate effort to recover deleted files from them.

***Method of Experiment*:** The experiment was carried out on the Maxtor HDD, Apple SSD, Samsung SSD, and the Maplin SSD with their respective specifications captured in Table 2. For the purpose of consistency, a total of 20 files where tested and they were selected to reflect variety and the total size of the files sums up to 1.54 GB.

The Maplin SSD and Maxtor HDD was formatted on the Windows 7 operating system with the NTFS file systems format while the internal SSD on the Apple MacBook Pro was formatted using the ExFat file systems format. After formatting all the 4 storage devices, the template files were used to populate the storage devices. The format operation was carried out to ensure that all the storage devices were at the same state at the time of writing the template files so that there will be consistency with the experimentation.

After populating all the drives with the template files, the delete operation was issued on all the 4 drives. After the delete process was completed, a forensic image of all the 4 storage media was made. The imaged files were then imported into FTK in order to find out the degree of recovery that can be made on all the drives and compare the relationships in terms of data retention even after deletion. The same method got repeated 3 times, the only difference became the time it took before the image was captured and setting off the recovery process. The time for capturing the image was marked at 1 minute, 30 minutes and 60 minutes.

2.2 Experiment 2: Hash Value Comparison

Purpose of Experiment: The hash value is regarded as the digital fingerprint of digital evidence. Using a write blocker as a device to ensure data is unaltered during imaging, then followed by computing the hash value has served as the forensic standard in which investigators utilize to demonstrate compliance. The purpose of this experiment is to compare the checksums value generated by the 4 storage devices used in the experiment and analyze their consistency when recomputed at a later time. The guidelines for non volatile memory forensic clearly stipulates that the hash value must always remain the same when recomputed because that is the only way to affirm the integrity of data domiciled in the storage media.

Method of Experiment: The experiment was carried out on the Maxtor HDD, Apple SSD, Samsung SSD, and the Maplin SSD with their respective specifications captured in Table 2. For the purpose of consistency, a total of 20 files where tested and they were selected to reflect variety and the total size of the files sums up to 1.54 GB.

The Maplin SSD and Maxtor HDD was formatted on the Windows 7 operating system with the NTFS file systems format while the internal SSD on the Apple MacBook Pro was formatted using the ExFat file systems format. After formatting all the 4 storage devices, the template files were used to populate the storage devices. The format operation was carried out to ensure that all the storage devices were at the same state at the time of writing the template files so that there will be consistency with the experimentation.

Thirdly, All the content of the 4 storage media was deleted and then FTK imager was used to make an image of the devices. At the final stage of the imaging procedure, a checksum value was created.

Lastly, to verify the checksum value which is usually the basis of admissible evidence in court, it will be recalculated after a waiting time of 1 hour then a comparison will be made to analyze any changes in the checksums.

2.3 Experiment 3: Impact of Trim on Evidence Recovery

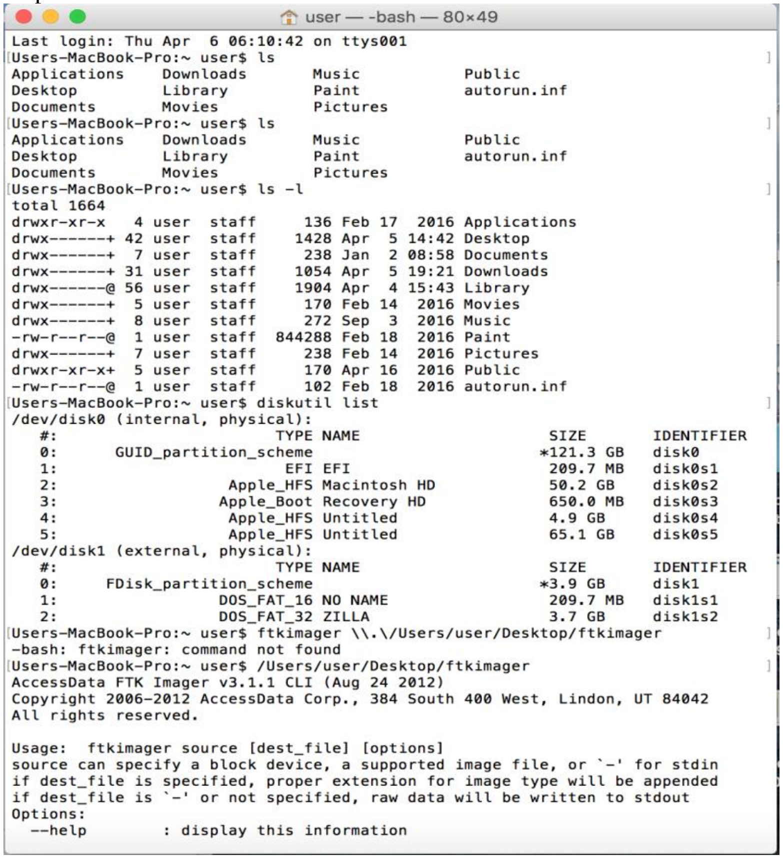
Purpose of Experiment: The purpose of this experiment is to determine if there will be any significant difference when the OS Trim function is disabled before evidence acquisition is carried out on the SSDs. The Trim function is a system of communication between the operating system and the SSD whereby, the operating system communicate with the SSD informing it of what particular data on what particular page can be over-written. In practice, the Trim command works like the disk defragmentation utility feature and for the Trim command to work, both the SSD and the Operating system must support the function. A paradigm of how the Trim command works in Windows Operating System is, when the SSD pronounces itself as having the Trim feature, Windows immediately disables disk defragmentation and enables the Trim command. When this communication pathway is recognized, seamless interaction between the SSD controller and the operating system can then be established (King and Vidas, 2011). Another important factor about the Trim command is that it can manually be enabled and disabled depending on the user's preference (Rouse, 2012).

Method of Experiment: This experiment was carried out on the three SSDs. The Apple SSD, Samsung SSD and the Maplin SSD. For the purpose of consistency, a total of 20 files were tested and the details of the files format is given in Table 2. The total size of the selected files sums up to 1.54 GB.

Using the procedure of disabling the Trim functionality giving in Fig 2, the Maplin SSD connected to the Windows 7 Operating System was disabled and using the procedure of disabling the Trim functionality documented in section in Fig 1, the Apple SSD and the Samsung SSD Trim function was disabled.

The three solid state drives are then formatted and populated with the sample data. After populating the three solid state drives, FTK Imager was used to capture the respective images keeping in mind that the OS Trim functionality has already been disabled before the images are captured.

Lastly, the Imaged files are imported into FTK for analysis to determine to what extent is the Trim functionality affecting the chances of evidence recovery.



```
Last login: Thu Apr  6 06:10:42 on ttys001
Users-MacBook-Pro:~ user$ ls
Applications    Downloads       Music           Public
Desktop         Library         Paint           autorun.inf
Documents       Movies          Pictures
Users-MacBook-Pro:~ user$ ls
Applications    Downloads       Music           Public
Desktop         Library         Paint           autorun.inf
Documents       Movies          Pictures
Users-MacBook-Pro:~ user$ ls -l
total 1664
drwxr-xr-x   4 user  staff     136 Feb 17  2016 Applications
drwx------+ 42 user  staff    1428 Apr  5 14:42 Desktop
drwx------+  7 user  staff     238 Jan  2 08:58 Documents
drwx------+ 31 user  staff    1054 Apr  5 19:21 Downloads
drwx------@ 56 user  staff    1904 Apr  4 15:43 Library
drwx------+  5 user  staff     170 Feb 14  2016 Movies
drwx------+  8 user  staff     272 Sep  3  2016 Music
-rw-r--r--@  1 user  staff  844288 Feb 18  2016 Paint
drwx------+  7 user  staff     238 Feb 14  2016 Pictures
drwxr-xr-x+  5 user  staff     170 Apr 16  2016 Public
-rw-r--r--@  1 user  staff     102 Feb 18  2016 autorun.inf
Users-MacBook-Pro:~ user$ diskutil list
/dev/disk0 (internal, physical):
   #:                       TYPE NAME                    SIZE       IDENTIFIER
   0:      GUID_partition_scheme                        *121.3 GB   disk0
   1:                        EFI EFI                     209.7 MB   disk0s1
   2:                  Apple_HFS Macintosh HD            50.2 GB    disk0s2
   3:                 Apple_Boot Recovery HD             650.0 MB   disk0s3
   4:                  Apple_HFS Untitled                4.9 GB     disk0s4
   5:                  Apple_HFS Untitled                65.1 GB    disk0s5
/dev/disk1 (external, physical):
   #:                       TYPE NAME                    SIZE       IDENTIFIER
   0:     FDisk_partition_scheme                        *3.9 GB     disk1
   1:                 DOS_FAT_16 NO NAME                 209.7 MB   disk1s1
   2:                 DOS_FAT_32 ZILLA                   3.7 GB     disk1s2
Users-MacBook-Pro:~ user$ ftkimager \\.\/Users/user/Desktop/ftkimager
-bash: ftkimager: command not found
Users-MacBook-Pro:~ user$ /Users/user/Desktop/ftkimager
AccessData FTK Imager v3.1.1 CLI (Aug 24 2012)
Copyright 2006-2012 AccessData Corp., 384 South 400 West, Lindon, UT 84042
All rights reserved.

Usage:  ftkimager source [dest_file] [options]
source can specify a block device, a supported image file, or `-' for stdin
if dest_file is specified, proper extension for image type will be appended
if dest_file is `-' or not specified, raw data will be written to stdout
Options:
  --help        : display this information
```

Fig. 1 Code Snippet FTK Imager for Mac OS X

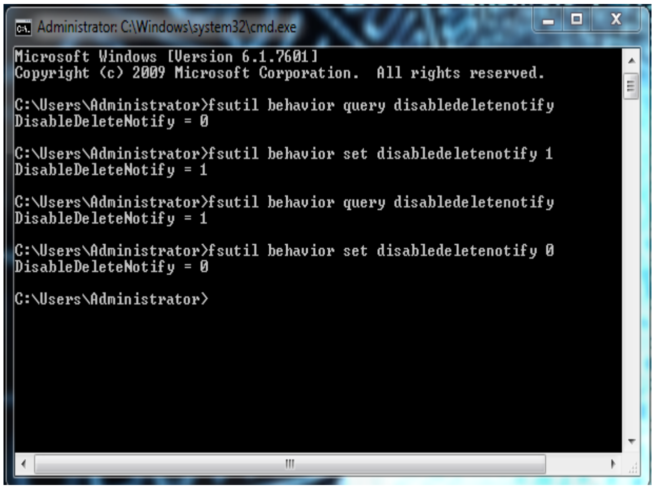
To enable or disable the SSD Trim function in Windows 7, the following command must be issued through the command prompt window.

Check Trim status: **fsutil behavior query disabledeletenotify**

Disable Trim Function: **fsutil behavior set disabledeletenotify 1**

Enable Trim Function: **fsutil behavior set disabledeletenotify 0**

Note: If the issued command returns a “0” then the Trim function is enabled and if it returns a “1” then the Trim function is disabled.



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

C:\Users\Administrator>fsutil behavior query disabledeletenotify
DisableDeleteNotify = 0

C:\Users\Administrator>fsutil behavior set disabledeletenotify 1
DisableDeleteNotify = 1

C:\Users\Administrator>fsutil behavior query disabledeletenotify
DisableDeleteNotify = 1

C:\Users\Administrator>fsutil behavior set disabledeletenotify 0
DisableDeleteNotify = 0

C:\Users\Administrator>
```

Fig. 2 Screenshot Enabling SSD Trim on Windows

2.4 Experiment 4: Recovery after Format Operation

Purpose of Experiment: The purpose of this experiment is to investigate whether there is a reasonable possibility of reconstructing digital evidence from formatted SSDs.

Method of Experiment: The experiment was carried out on three SSDs, the Apple SSD, Samsung SSD and the Maplin SSD with all the specification in table 2.

After formatting all three SSDs, the template files were used to populate the storage devices. The format operation was carried out to ensure that all the storage devices were at the same state at the time of writing the template files so that there will be consistency with the experimentation.

After populating all the drives with the template files, the format operation was issued on all three SSDs. Furthermore, the forensic image of all the storage media was made. The imaged files were then imported into FTK in order to find out the degree of recovery that can be made on all the drives and compare the relationships in terms of data retention even after the format operation.

3. Results and Discussions

From the results of the experimentation, dependable conclusions will be established based on the findings and that in effect will shape the approach applicable for the most effective and reliable SSD forensics.

3.1 Result and Discussion of Experiment 1

Table 4: Result of Experiment 1

SN	***Storage Media***	***Tested Files***	***Recovered Files[Minutes]***	***Avera ge***	**%**
1	Maxtor HDD 80GB	20	20 in 1 Mins 20 in 30 Mins 20 in 60 Mins	20.00	100.00
2	Apple SSD 128GB	20	20 in 1 Mins 17 in 30 Mins 15 in 60 Mins	17.33	86.65
3	Samsung SSD 250GB	20	7 in 1 Mins 0 in 30 Mins 0 in 60 Mins	2.33	11.65
4	Maplin SSD 256GB	20	6 in 1 Mins 0 in 30 Mins 0 in 60 Mins	2.00	10.00

The results in Table 4 shows that HDDs are architecturally different from SSDs and more forensically friendly for recovering deleted files. However, it is apparent for forensic analysts to never assume equality of the two kinds of storage media and impose the HDD forensic methods on the SSDs even though both are non volatile in nature. For the three SSDs, there is an aggressive non uniformity in their reaction to identical forensic procedures. Close investigation suggests a major factor called Garbage Collection which could be responsible for the low recovery rate especially in the Samsung and Maplin SSDs.

Garbage Collection*:* By definition, garbage collection (GC) is a process which involves identifying and clearing blocks of unnecessary data so that space can be created for the allocation of new data (Shahidi et al., 2016). The need for high efficiency in SSDs is the reason for the implementation of the garbage collection routine, because of the high latency involve in delete operations which, if concurrently carried out with other SSD operations will significantly impact on the performance. The constant and random movement of data on SSDs to allow the controller carry out the GC routine causes the volatility of the data. Furthermore, the freedom of SSD manufacturers to implement the GC algorithm however they please effectively transpose into undiscerned fluidity in the behavior of the SSD. This primarily explains the inconsistency of the recovered data across the SSDs because, the GC routine is in total obedience to how they are programmed.

3.2 Result and Discussion of Experiment 2

Table 5: Result of Experiment 2

SN	***Storage Media***	***Hash Value MD5 Checksum()***	***Recomputed Hash***
1	Maxtor HDD 80GB	02ec6e359b57b337ca81fd1fd3bf409c	02ec6e359b57b337ca81fd1fd3bf409c
2	Apple SSD 128GB	32a9652272f18105daa11f83845247f9	32a9652272f18105daa11f83845247f9
3	Samsung SSD 250GB	0bade5cddc99fefaec3f6daa5439f10e	0bade5cddc99fefaec3f6daa5439f10e
4	Maplin SSD 256GB	43acfac478e94890406f7f44289d239f	33ec4b727b7169d930d70c6c1db471b0

The hash value is regarded as the digital fingerprint of digital evidence. Using a write blocker as a device to ensure data is unaltered during imaging, then followed by computing the hash value, has served as the forensic standard in which investigators utilize to demonstrate compliance (John, 2014). From the result of experiment 2 which is captured in Table 5, the Maplin SSD returns different checksums when ever it is recomputed and close investigation into the causative factor discloses **wear leveling** to be the reason for the hash value inconsistency.

Wear Leveling: This is an SSD feature that improves cell longevity by managing data distribution equally across the whole drive. Wear leveling makes use of an algorithm to ensure that all write operations are kept even across the flash chips so that the overall life span of the device can be prolonged. The algorithm embedded in the SSD firmware ensures that the controller remaps all logical block addresses to various physical block addresses in the solid state memory array. Without wear leveling, the flash memory cells can only endure a finite number of write/delete cycles before they experience total wear. This efficiency design decision in SSDs partly closes the forensic window of opportunity exploited by experts because, wear leveling does not need any form of express permission from a user to execute hence, absolute self corrosiveness of SSDs cannot be avoided. Just like GC, manufacturers have the liberty to determine how they want to implement wear leveling on their SSDs. This explains why Apple and Samsung SSDs retained their checksum values in the experiment because they have lower frequency of the time needed for routine wear leveling operation as oppose to the Maplin SSD.

Table 6: Result of Experiment 3

SN	***Storage Media***	***Tested Files***	***Recovered Files***	**%**
1	Apple SSD 128GB	20	20	100.00
2	Samsung SSD 250GB	20	20	100.00
3	Maplin SSD 256GB	20	16	80.00

From the findings of experiment 3 with corresponding result captured in Table 6, it shows that there is a clear indication that disabling the operating system Trim functionality significantly improves the chances of recovering deleted data from SSDs. So it should be a good practice for forensics analysts to always disable operating system Trim function on supported SSDs as the chances of recovering data are far more plausible.

Table 7

SN	***Storage Media***	***Tested Files***	***Recovered Files***	**%**
1	Apple SSD 128GB	20	0	0.00
2	Samsung SSD 250GB	20	0	0.00
3	Maplin SSD 256GB	20	0	0.00

The three solid state drives behaved identically when this experiment was conducted. There was 0.00% recovery of the formatted SSDs which was not farfetched from the prediction of (Gubanov and Afonin, 2016). From the FTK analysis toolkit, most of the partition of the solid state drives was zeroed out to depict that there is essentially no data that can be carved out from slack space which when dealing with SSD, it is referred to as the minimum writable and minimum erasable blocks on a physical level. The only trace of data from the toolkit is the file systems format of the solid state drive.

4. Conclusion

This work provided contextual clarity to the stochastic nature of the SSD architecture and postulates the most effective maneuver for digital evidence acquisition. This study clearly shows that the widely acceptable approach for HDD forensics cannot and should not be imposed on SSDs just because they are both non volatile in nature. The flexibility enjoyed by SSD manufacturers should inform the specific approach used by forensic experts because the series of experiments conducted revealed that the SSD controller implements garbage collection, wear leveling and Trim functionality differently and knowing these key factors, goes a long way in determining the success rate of the analysis.

With over 224.1 million units of SSDs shipped worldwide, and more than 40% of the HDD market being replaced by SSDs it is critical that forensic experts come to grips with this technology and make deliberate effort to refine their non volatile memory forensic approach.

References

[1] Bonetti, G., Viglione, M., Frossi, A., Maggi, F. and Zanero, S. (2014). Black-box forensic and antiforensic characteristics of solid-state drives. Journal of Computer Virology and Hacking Techniques, 10(4), pp.255-271.

[2] Casey, E. (2011). Digital evidence and computer crime. 3rd ed. Waltham: Academic Press.

[3] John, B. (2014) "SSD Architecture and Function", Forensic Magazine. Available at: http://www.forensicmag.com/article/2014/06/solid-state-drives-part-6 (Accessed: 19 March 2017).

[4] King, C. and Vidas, T. (2011). Empirical analysis of solid state disk data retention when used with contemporary operating systems. Digital Investigation, 8, pp.S111-S117.

[5] Micheloni, R., Marelli, A. and Eshghi, K. (2012) Inside solid state drives (SSDs). Netherlands: Springer.

[6] Nelson, B., Phillips, A. and Steuart, C. (2016). Guide to computer forensics and investigations. 1st ed. Boston: Cengage Learning.

[7] Rouse, M. (2012) What is TRIM?, SearchSolidStateStorage. Available at: http://searchsolidstatestorage.techtarget.com/definition/TRIM (Accessed: 26 March 2017).

[8] Shahidi, N., Kandemir, M., Arjomand, M., Das, C., Jung, M. and Sivasubramaniam, A. (2016) "Exploring the Potentials of Parallel Garbage Collection in SSDs for Enterprise Storage Systems", SC16: International Conference for High Performance Computing, Networking, Storage and Analysis. doi: 10.1109/sc.2016.47.

[9] Shey, J., Rakvic, R., Ngo, H., Walker, O., Tedesso, T., Blanco, J.A. and Fairbanks, K. (2016) 'Inferring trimming activity of solid-state drives based on energy consumption', 2016 IEEE International Instrumentation and Measurement Technology Conference Proceedings,. doi: 10.1109/i2mtc.2016.7520537.

[10] Sibiya, G., Venter, H. S., Ngobeni, S., and Fogwill. (2012) "Guidelines for procedures of a harmonised digital forensic process in network forensics," Information Security for South Africa (ISSA), 2012, Johannesburg, Gauteng, 2012, pp. 1-7.

[11] Smith, J. (2005) What is an SSD? Available at: https://www.quora.com/What-is-an-SSD-1#!n=18 (Accessed: 10 July 2019).

Authors –

Song Shombot Emmanuel graduated from the University of East London with a Bachelor's degree in Software Engineering in 2012 and a Master's degree in Information Security and Digital Forensics in 2017. He is currently working as a Lecturer in Federal University Lafia, Nigeria. S.S. Emmanuel has been a constant recipient of the Dean's list award of academic excellence in 4 consecutive semesters during his Undergraduate years and also won the Tertiary Education Trust Fund Award (TETFUND in 2016. The author's current research interest is IoT and Big Data Analytics.

Dr. Ameer Al-Nemrat is a senior lecturer at the School of Architecture, Computing and Engineering, University of East London (UEL). He also the Director of Professional Doctorate in Information Security & the MSc Information Security and Digital Forensics programmes. In addition, Ameer is the founder and the director of the Electronic Evidence Laboratory, UEL. Ameer is a research active in the area of cybercrime and digital forensics where he has been publishing research papers in peer-reviewed conferences and internationally reputed journals. He is a co-editor of the book "Issues in Cybercrime, Security, and Digital Forensics". He also was the guest editor of the special issue of the International Journal of Electronic Security and Digital Forensics (IJESDF). Ameer has led a Cybercrime Programme Project with a German institution, which won for the second time in a row, the "Good Practice Award" from The European Commission under the Leonardo da Vinci scheme which focuses on the teaching and training needs of those involved in vocational education and training." Ameer was also nominated as the "Best Lecturer" for 2015 - Student Led Teaching Awards – Spotlight on Great Teaching 2015.

Shehu Mohammed Ahmed is a graduate from Federal University of Technology Minna with bachelor's of Technology in Mathematics and Computer Science 2010 and Master's of Technology in Mathematics 2016. He is currently working as Lecturer in Department of Computer Science Federal University of Lafia.
The Authors current research area is Algorithms and Computational mathematics