

**St. Cloud State University
theRepository at St. Cloud State**

Culminating Projects in Information Assurance

Department of Information Systems

3-2019

Analyzing the Trimming Activity of Solid-State Drives in Digital Forensics

Shoban Kandala

skandala@stcloudstate.edu

Follow this and additional works at: https://repository.stcloudstate.edu/msia_etds

Recommended Citation

Kandala, Shoban, "Analyzing the Trimming Activity of Solid-State Drives in Digital Forensics" (2019). *Culminating Projects in Information Assurance*. 81.

https://repository.stcloudstate.edu/msia_etds/81

This Starred Paper is brought to you for free and open access by the Department of Information Systems at theRepository at St. Cloud State. It has been accepted for inclusion in Culminating Projects in Information Assurance by an authorized administrator of theRepository at St. Cloud State. For more information, please contact rswexelbaum@stcloudstate.edu.

Analyzing the Trimming Activity of Solid-State Drives in Digital Forensics

by

Shoban Kandala

A Starred Paper

Submitted to the Graduate Faculty of

St. Cloud State University

in Partial Fulfillment of the Requirements

for the Degree of

Master of Science

in Information Assurance

March, 2019

Starred Paper Committee:
Mark Schmidt, Chairperson
Dennis Guster
Sneh Kalia

Abstract

The primary source for storing digital information has been remained constant for the last two decades, in the form of magnetic disks. However, a sudden shift has taken place in the data storage technology during the recent years where the transistor-based devices are being used as primary storage devices for storing complex data. There are many reasons due to which the manufacturers are shifting their platform from magnetic disks to solid state drives which uses transistor chips and this change is creating problems for the forensic investigators to investigate on the digital evidence.

The deleted information can be easily retrieved from the hard disks by following specific guidelines, where as in solid state drives it is almost impossible to retrieve the lost data when TRIM command is enabled. SSDs can sometimes sanitize data all by themselves even if they are not connected to any interface. This paper gives an overview of the hard disks and solid-state drives for data recovery and mainly focuses on the functioning of TRIM command in solid state drives.

Table of Contents

	Page
List of Tables	6
List of Figures	7
Chapter	
I. Introduction.....	10
Introduction.....	10
Problem Statement.....	12
Nature and Significance of the Problem	12
Objective of the Study	113
Study Questions	13
Limitations of Study	13
Definition of Terms.....	14
Summary.....	15
II. Background and Literature Review	16
Introduction.....	16
Background Related to Problem	16
Literature Related to Problem	17
Forensics	17
Digital Forensics	17
Forensic Process.....	18
Hard Disk Drives	18

Chapter	Page
Solid State Drives	23
Literature Review Related to the Methodology	32
Functioning of a Drive with TRIM and without TRIM	32
TRIM Function in Windows Operating System	34
III. Methodology	35
Introduction.....	35
Design of Study.....	35
Data Collection	36
Tools and Techniques	36
Hardware and Software Requirements	36
Timeline	37
IV. Data Presentation and Analysis	38
Introduction.....	38
Data Presentation	38
Installation of FTK Imager	38
Forensic Toolkit (FTK).....	44
Key Files of Interest.....	48
Solid State Drive	48
Data Analysis	51
Hard Disk Drive Image	51
Performing the Analysis by Erasing the Data from Hard Disk Drive	60

Chapter	Page
Analysis on Hard Disk Drive	60
Analysis on Solid-State Drive.....	62
Summary	64
V. Results, Conclusion and Recommendations	65
Introduction.....	65
Results.....	65
Conclusion	67
Future Work	67
References.....	68

List of Tables

Table	Page
1. Improvements of HDD Characteristics Over Time	19
2. Static vs. Dynamic Wear-Leveling Methods	29

List of Figures

Figure	Page
1. Hard Disk Drive and Solid-State Drive	11
2. Forensic Analysis Process.....	18
3. Components of a Hard Disk Drive.....	21
4. Hard Disk Tracks and Cylinders.....	22
5. NAND Flash Cell.....	24
6. Components of Solid-State Drive	25
7. Hierarchy of the Flash Chip Architecture	26
8. Garbage Collection Process	30
9. TRIM.....	31
10. SSDs Can Only Be Erased One Whole Block at a Time.....	32
11. Garbage Collection with TRIM	33
12. Installation Page for FTK Imager	39
13. Details Page to Download the FTK Imager	39
14. Download Confirmation Page.....	40
15. Confirmation Email from Access Data.....	40
16. InstallShield Wizard for FTK Imager	41
17. First Step of Installation Wizard	41
18. User License Agreement for Access Data Software.....	42
19. Selecting the Destination Folder for Installation	42
20. Selecting the Destination Folder for Installation	43

Figure	Page
21. User Interface for FTK Imager	43
22. Access Data Website Which Shows the Forensic Toolkit Version to Download	44
23. Forensic Toolkit Installer Window	45
24. Forensic toolkit InstallShield Wizard	45
25. License Agreement Window for Forensic Toolkit	46
26. Setup Type Window for Installing Toolkit.....	46
27. Progress of Installation for FTK Suite	47
28. Completion of Installation for FTK Suite	47
29. External Hard Disk rive Connected to the Laptop.....	48
30. Folders and Files in the Hard Disk Drive	48
31. Internal SSD Connected Externally to a System Using ESATA Port	49
32. Displaying Disk Allocated Space and Use Space for Solid-State Drive	49
33. File and Folders in the Solid-State Drive.....	50
34. Image Displaying the Free and Allocated Space in the Solid-State Drive	50
35. Window Displaying the FTK Imager	51
36. Loading the Logical Drive to Create an Image.....	52
37. Selecting the Appropriate Drive to Create the Image	52
38. Adding a Destination Location to Save the Image	53
39. Selecting the Destination Image Type	53
40. Evidence Item Information	54
41. Giving a Specific Image File Name	54

Figure	Page
42. Window Displaying the Image Creation in Progress.....	55
43. Window Displaying the Image Creation Completion.....	55
44. Access Data's Forensic Toolkit Wizard for Adding Evidence to the Case	56
45. File Type Selection to perform the Image Mounting.....	56
46. Adding Acquired Image as Evidence	57
47. Adding Acquired Images from the Local Destination	57
48. Providing the Evidence Information for the Image	58
49. Setup Completion Window.....	58
50. Forensic Toolkit Processing the Files	59
51. Files Retrieved from the Mounted Images.....	59
52. Erased Hard Disk Drive	60
53. Command Prompt Running as an Administrator and Query to Show the Status of the TRIM on the System.....	60
54. TRIM Command Set to the Disabled Status.....	61
55. Command Prompt with TRIM Status Enabled	61
56. Image Showing the Results for Hard Disk Drive	62
57. Mounting the Solid-State Drive to Perform Analysis.....	62
58. Evidence Item Information	63
59. Selecting the Image Destination	63
60. Creation of Image in Progress.....	64

Chapter I: Introduction

Introduction

The current generation of computer technology and internet has created a huge impact on the society. The computers have become a part of life and are being used in every field such as banking, industry, shopping, communication, etc. There are wide variety of methods employed for storing the user information and one of the most common devices is hard disk drive which uses magnetic media to store the information.

For several years, hard disk drives played a crucial role in the computer technology. Recently, manufacturers are trying to improve reliability, speed of data access and high-power consumption in the computing devices (Boddington, 2010). To overcome these factors, the manufacturers are shifting towards solid state drives. The hard disk drives rely on multiple plates rotating on a spindle within a protective casing and stores data magnetically, whereas the solid-state drives are built from semiconductor chips and have no rotating parts, are compact in size and more economical of power consumption.

These hard disk drives and solid-state drives play a crucial role in the field of forensic investigation. Along with change in the technology, criminals also adopted new technologies and developed strategies to commit crimes. This shift in technology required forensic investigators to design new approaches for collecting evidences from the storage devices (Kopchak, 2016). Typically, the file which has been marked as deleted in the hard disk drives will still be present in the space associated with the file and is returned to the pool of available storage. By understanding this procedure, one can easily recover deleted files from the magnetic drive. This basic property of magnetic drive has become key for forensic investigations.

On the other hand, the solid-state drives are creating problems for the forensic investigators. Unlike magnetic drives, the solid-state drives use wear-levelling technique and once the file is deleted, SSDs can empty all sector within the drive at all time making it new thus obscuring to recover deleted files (Hubbard, 2016). Many manufacturers have chosen to increase the reliability of 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 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 (Fulton, 2014).

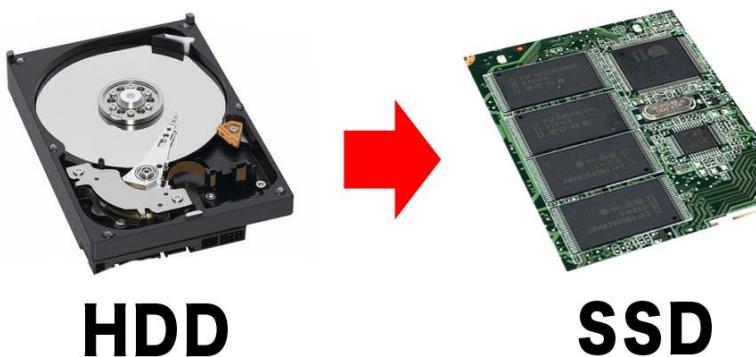


Figure 1: Hard Disk Drive and Solid-State Drive (Draalin, 2013)

In recent times, the manufacturers are ensuring the data to be re-written on the drive consistently and hence they have enabled the TRIM function. When a file is given a delete operation, TRIM ensures that it erases the file from the SSD memory, and the data overwritten is executed consistently. The features garbage collection, self-corrosion also ensures that the file is permanently erased in the background of the sector within few minutes. Hence in SSDs, the deleted data will be lost forever in the matter of minutes. If we try to shut down the computer after the command is issued, it will not stop the destruction. This self-destruction is triggered by

TRIM command issued by the operating system to the SSD controller at the time the user deleted the file, formats the disk or deletes the partition (Yuri Gubanov, 2014). In this paper, we will try to analyze the consequences when the TRIM value is changed from ‘0’ to ‘1’ on the operating system and will evaluate the results based on the output.

Problem Statement

Digital forensics is mainly dependent on computer forensic investigations where digital media is used to solve the cases. The forensic investigators have well defined procedures for solving the cases using hard disk drives. However, due to sudden shift in the technology, the solid-state drives have come into existence replacing the magnetic drives. Due to its unique storage procedures, the users started committing crimes using solid-state drives.

Retrieving deleted files from the SSDs have become a nightmare for the forensic investigators. In SSDs, once the delete command is given, file is completely erased from the SSD memory using TRIM function. Considering this TRIM function, there are few questions that need to be answered like: Is there any way that the TRIM function can be disabled and What happens to the deleted files if this TRIM function is disabled? Can we retrieve the deleted files while disabling the TRIM function? In this paper, we will discuss the problems faced by the forensic investigators when a file is deleted from the SSD and the consequences faced by the SSD while the TRIM function is changed.

Nature and Significance of the Problem

The advanced techniques and procedures that were followed by forensic investigators to solve the cases using hard disk drives are no longer possible using modern solid-state drives. This has become a serious issue while solving the complex cases. As per recent study, SSDs

production in 2009 was 11 million units and it has increased to 227 million units in 2017 (Solid State Drives [SSD], n.d.). This shows that the production of SSDs has been increased 20 times within 8 years and if this is the case, would it be impossible to solve the cases using digital forensics? In this paper, we would be deducing on the cases on which the files can be retrieved from SSDs.

Objective of Study

The main objective of study is to find out why the forensic investigators are facing troubles while trying to recover the lost data from the solid-state drives. This study will also compare the results by following the same set of procedures on the operating system and changing the TRIM value.

Study Questions

The study questions may constitute like:

1. What are the difficulties caused by the forensic investigators while using SSDs?
2. Can the files in the drive be recovered if the TRIM command is disabled on the operating system?
3. What difference makes the TRIM functionality on an SSD to an acquisition process?

Limitations of Study

The focus of this report will be on the difficulties faced by the forensic investigators to recover the lost data from the SSDs. This study will not attempt to make any changes in the current data recovery procedures or methods that are being used by the forensic investigators. However, this study will show a case study wherein the lost data can be recovered from an SSD by modifying the TRIM function.

Definition of Terms

Hard disk drives: A hard disk drive is a data storage device that uses magnetic storage to store digital information using one or more rotating disks coated with magnetic material (Hard Disk Drive [HDD], n.d.). The platters are paired with magnetic heads, usually arranged on a moving actuator arm, which read and write data to the platter surfaces. In this the data can be accessed in a random – accessed manner that means individual blocks of data can be stored or retrieved in any order and not only sequentially.

Solid state drives: A solid-state drive (SSD) is a solid-state storage device that uses integrated circuit assemblies as memory to store data persistently. SSD technology primarily uses electronic interfaces compatible with traditional block input/output (I/O) hard disk drives (HDDs), which permit simple replacements in common applications. SSDs have no moving mechanical components (Solid State Drives [SSD], n.d.). Compared with electromechanical disks, SSDs are typically more resistant to physical shock, run silently, and have lower access time and lower latency.

Digital forensics: Digital forensics is a branch of forensic science encompassing the recovery and investigation of material found in digital devices, often in relation to computer crime. The term digital forensics was originally used as a synonym for computer forensics but has expanded to cover investigation of all devices capable of storing digital data. Digital forensics investigations have a variety of applications (Digital Forensics, n.d.). The most common is to support or refute a hypothesis before criminal or civil courts.

TRIM command: A trim command allows an operating system to inform a solid-state drive which blocks of data are no longer considered in use and can be wiped internally

(Intel.com, 2017). Trimming enables the SSD to more efficiently handle garbage collection, which would otherwise slow future write operations to the involved blocks.

Garbage collector: The Garbage collector works closely together with the TRIM functionality. It keeps track of the to be deleted cells and can combine leftover data of different cells to empty ones to delete others (Geier, 2015). This fully works in the background and can only be suspected to work along with TRIM.

Summary

In this chapter, we learned about the hard disk drives and solid-state drives and their design in brief. Also, we have seen how HDDs are different from modern SSDs and why they are being manufactured in large number. Due to increase in large number of SSDs, the users are taking this as an advantage and committing crimes and this has become a difficult task for the forensic investigators. Throughout the years, forensic investigators have followed certain methods to recover lost data from the magnetic drives and why are they now facing difficulties in doing the same with the modern solid-state drives? A brief description of all the main terms used in for this report have been discussed in the above context. Finally, we have mentioned about TRIM function and garbage collector and how do they affect the process of recovering lost data from a solid-state drive. In the next chapter, we will be discussing the main problem of SSD and the operation of both HDD and SSD.

Chapter II: Background and Literature Review

Introduction

Most of the digital forensic investigations are solved using the storage devices because the crimes are mostly done using the computer technology. The main component of these computers is their storage devices which in this case is hard drives and solid-state drives. Gathering lost data from hard drives is a common task followed by the forensic investigators throughout the years but recovering the lost data from the solid-state drives have become a difficult task for them. Why is the recovering process different in solid state drives when compared with hard drives? To find out the reason, we must learn how both the drives function and how the data is stored in each drive and role of each drive in forensic investigations. In this chapter, we will be discussing the concepts on how both the drives store information, their functioning, use in digital forensics and role of TRIM function is SSDs.

Background Related to Problem

The most common problem faced by the forensic investigators in recent times is how to retrieve lost data from the solid-state drives. The hard drives used to store the deleted information whereas the solid-state drives are not able to store the data. This is because, the solid-state drives have special characteristics called as garbage collector and TRIM function which could completely erase the deleted information from the storage. So, we will be learning in detail about the functioning of SSDs and HDDs and their role in digital forensics.

Literature Related to Problem

Forensics

Forensics is a scientific method of gathering and examining information about the past which is then used in the court of law. This evidence is collected to find out the link between the suspect and the crime. To provide a reliable evidence, it involves three concepts: chain of custody, Admissibility of tests, evidence and testimony and expert witness.

The chain of custody describes the documentation and evaluation of the evidence. By using these documents, the evidence can be carefully studied at again and again at any time. This document should also notify the time and location where it is being stored from the time of documentation till date. Admissibility of Tests, Evidence and Testimony involves the existence of legal standards for the admissibility of forensic tests and expert testimony (Geier, 2015). Expert Witness Relating to all forensic science disciplines is the third issue, the concept of the expert witness. In an investigation of any kind there can be a fact witness, who can usually only relate facts that the person observed, and an expert witness.

Digital Forensics

Digital forensics can be defined as:

The use of scientifically derived and proven methods toward the preservation, collection, validation, identification, analysis, interpretation, documentation, and presentation of digital evidence derived from digital sources for facilitation or furthering the reconstruction of events found to be criminal or helping to anticipate unauthorized actions shown to be disruptive to planned operations. (DFRWS, 2001, p. 16)

Digital forensics has become prevalent because law enforcement recognizes that modern day life includes a variety of digital devices that can be exploited for criminal activity. To know how the drives are used for forensic investigations, we must study the forensic process.

Forensic Process

A digital forensic process mainly consists of three phases: acquisition or imaging of exhibits, analysis and reporting. Acquisition generally is capturing an image of the RAM and creating a duplicate of the media using write blocking device. However, the data now-a-days is being stored in the cloud, so a logical copy of data is taken instead of complete image of storing device. During the analysis phase an investigator recovers evidence material using different methodologies and tools (Digital Forensics, n.d.). The actual process of analysis can vary between investigations, but common methodologies include conducting keyword searches across the digital media (within files as well as unallocated and slack space), recovering deleted files and extraction of registry information (Digital Forensics, n.d.). When an investigation is completed the data is presented, usually in the form of a written report.

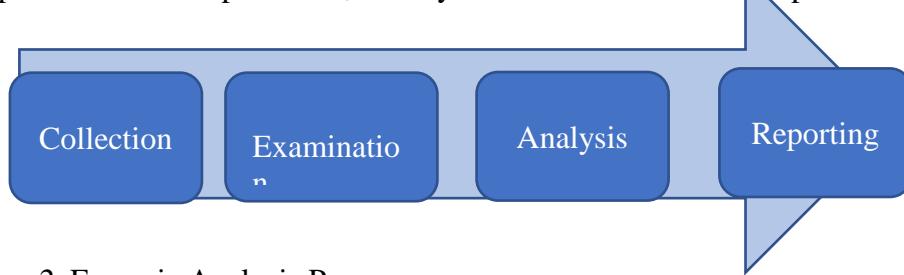


Figure 2. Forensic Analysis Process

Hard Disk Drive

HDD background. Hard drives are introduced in 1956 as data storage devices for IBM real-time transaction processing and are mainly used for mainframe and minicomputers. The first IBM drive, the 350 RAMAC in 1956, was approximately the size of two medium-sized

refrigerators and stored five million six-bit characters (3.75 megabytes) on a stack of 50 disks (IBM, 2015). Later in 1962, IBM 1301 disk storage was introduced which consists of 50 platters each about 1/8-inch thick and 24 inches in diameter. The technology used in IBM 350 is still used in the hard drives manufactured today. Today's desktop drives spin with a speed of 7,200 rpm and store up to 6 terabytes of data. The internal cable has changed from Serial to IDE (Integrated Drive Electronics) to SCSI (Small Computer System Interface) and finally SATA (Serial ATA) over the years.

Table 1

Improvements of HDD Characteristics Over Time

Parameter	During 1956	During 2015- 2017
Capacity	3.75 megabytes	14 terabytes
Physical Volume	68 Cubic feet (1.9 m ³)	2.1 Cubic inches (34 cm ³)
Weight	2000 Pounds (910 Kg)	2.2 Ounces (62 g)
Access Time	600 milliseconds	2.5ms to 10ms
Price	US\$9,200 per megabyte	US\$0.032 per gigabyte
Data Density	2,000 bits per square inch	1.3 terabits per square inch

(Hard Disk Drive, n.d.)

HDD mechanism. Basically, hard disk is one of the valuable components of a computer which stores all the data and is also the part that holds up the entire computer from operating as fast as it could. This hard disk is basically slow because of its moving mechanical parts and each moment takes some time. To know how a hard disk works, we must know about all the components present inside the disk. Usually, hard disks comprise of many parts, sealed in a dust free chamber to ensure correct drive operation.

On HDD, data is recorded on a spinning disk called platter and is head reads or writes the stored data. An actuator is used to regulate the position of head and the slider. The platter rotates from 4,200 rpm in energy efficient portable drives to 15,000 rpm for high end performance drives. To save the data on HDD, physical and logical formats are required. The physical format is also called as low-level formatting which divides a platter surface to basic entities of tracks, sectors and cylinders. The purpose of the physical format is to prepare the platter surface to be written on and for manufacturer to identify defective sectors.

The logical format is also called as high-level formatting which creates a file system on the platter. The file system is used by an HDD to access, read and write data on the operating systems. Storage area can be divided into partitions if multiple file systems are required on the hard disk. The main function of file system is to define an allocation table to efficiently access the data without searching the entire storage space.

HDD components. The basic components of hard drive are:

- *The Platter* which is a metal alloy disk coated with aluminum and is used to store all the information. All your data is stored using magnetic polarity differences.
- *The Spindle and Drive Motor* is a component which drives the spinning disks and the spinning speed could be distinct for HDDs within different product lines. When the disk is spinning, the sliders fly on a formed air-bearing surface. The faster the platters rotate, the faster the read/write head can obtain data. This component uses ball bearings and is one of the most sensitive components in a hard disk.
- *The Read-Write Heads:* The heads are responsible for reading and writing data to the drive. They write data by arranging the magnetic particles on the surface of the

platters. When arranged in one direction, the particles will represent a 0 and when arranged in the other direction, they will represent a 1 (Data Recovery, 2014). When reading from the platters, the head will detect the polarity of the particles and translate that into electrical signals and send the signals back to the on-board hard drive controller.

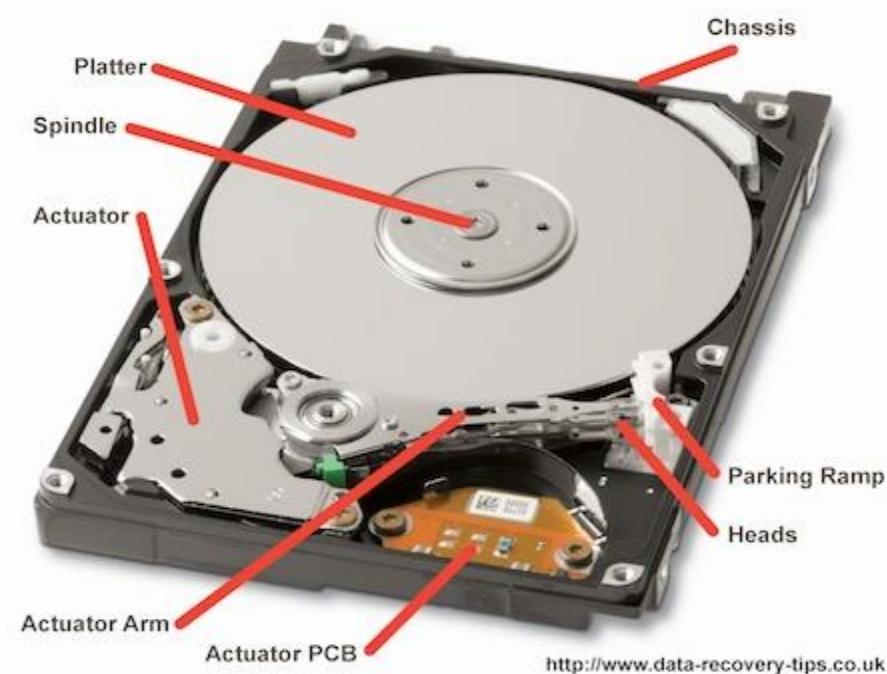


Figure 3. Components of a Hard Disk Drive (Hard Disk Drive, n.d.)

- *The Controller Board:* This contains several chips to regulate the data flow across the drive. This is attached to the hard drive chassis.
- *The Magnets:* The actuator contains two strong magnets one above and underneath it. The magnetic field on the magnets lie on a vertical axis and it will not affect the platters.

- *The Chassis:* Chassis is a component used to hold all the components firmly in place so that there are no vibrations while running.

Arrangement of data on hard disks. The data in the hard disk is arranged in the form of bits and the smallest data that can be accumulated on a disk is 1 bit. These bits are arranged in the circular forms around the disk. Typically, a hard drive contains around 70,000 to 100,000 tracks on each surface (Geier, 2015). All the data in the disk is written in the form of 512 bytes along the track. After one track is written and if the data to be written on the different track, the write head is moved by the arm to the next position on the radius.

A separate head is used for each surface of the disk and all heads have same position on its according surface. All the outer track surfaces are referred as 0, so all the outer surface tracks are called cylinder 0 (Abdullah Al Mamun, 2007). Each track is divided into sectors called as servo sectors. Each sector is typically 512 bytes and addressed starting from 1 on each track.

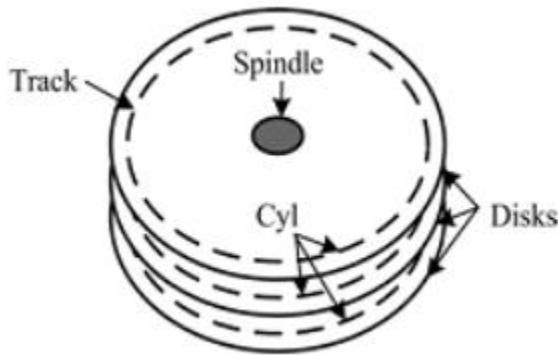


Figure 4. Hard Disk Tracks and Cylinders (Abdullah Al Mamun, 2007)

Solid State Drives

A solid-state drive is a storage device which emulates hard disk drive but is made up of semiconductor components. These drives are designed to replace the magnetic hard drives. The

working principal of solid-state drives is completely different from that of hard disks. These solid-state drives have no moving parts and are designed to benefit the end user. These drives will operate with their existing operating systems and hardware without any additional effort. However, since the technologies and principals used in this drive are different, the techniques for retrieving the evidence also need to be changed simultaneously. Solid-state drive uses nonvolatile memory as its storage media. Both the HDD and the SSD are part of a class of storage called block devices. These devices use logical addressing to access data and abstract the physical media, using small, fixed, contiguous segments of bytes as the addressable unit (Blackburn, 2012).

NAND flash cell. The NAND flash is made from floating gate transistor. This flash cell is made up of a circuit and is designed to store information. Electrical charge is stored on the floating gate which is isolated above and below by oxide insulating layers. In its simplest form when the floating gate is charged, it is programmed and recognized as a binary 0 (Cactus Technologies, 2017). When the floating gate has no charge, it is erased and recognized as a binary value of 1.

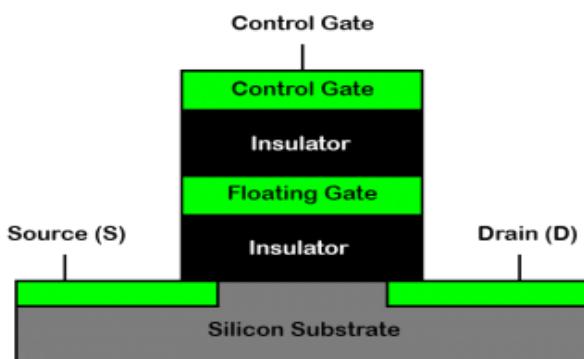


Figure 5. NAND Flash Cell (Cactus Technologies, 2017)

To read the cell, voltage is applied to the control gate and current flow from source to drain is attempted. If there is no current flow, it shows that the floating gate is charged (binary 0) and if the current is passed, the floating gate is not charged (binary 1) (Cactus Technologies, 2017). To write to a NAND cell, a high voltage is applied to the control gate and electrons move from silicon substrate to the floating gate. This process is called tunneling since the electrons tunnel through the oxide insulator to reach the floating gate. A single flash cell would not be of much value. So many flash cells are arranged in the form of a string to store large amount of data. NAND cells can usually store 32 bits of data, which still translates into 4bytes of data, so the strings are combined to form an array to achieve large storage of data.

SSD components. Each block device consists of three major parts: storage media, a controller for managing the media, and a host interface for accessing the media

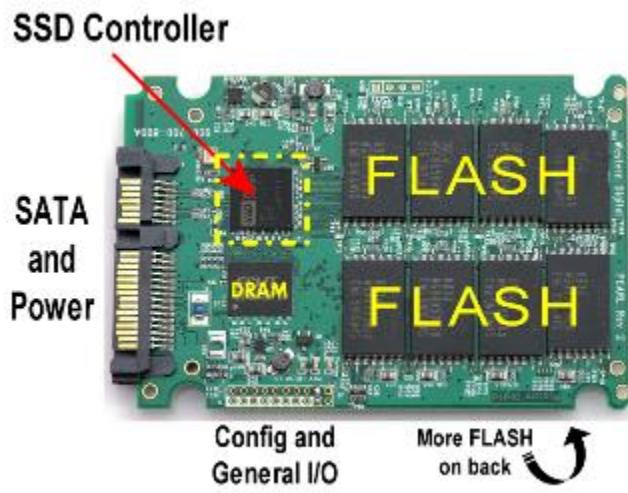


Figure 6. Components of Solid-State Drive (Rent, 2010)

NAND flash chips: SSDs are made up of NAND flash memory chips with data read and written on the disk. Flash memory is a non-volatile computer storage technology that can be electrically erased and reprogrammed. Flash memory offers fast read access times and better

kinetic shock resistance than hard disks. NAND flash uses floating-gate transistors, but they are connected in a way that resembles a NAND gate (Choi, 2010). A NAND flash chip consists of cells, pages, blocks and planes each with their own physical properties can be committed (a delete-before-write operation), and erase operations take much longer than a write, so designers needed a way to minimize the impact of this operation while maintaining wear leveling (Nitin Agrawal*, 2002). The controller needs to maintain number of active pagers for writing, so that the garbage collector running in the background finding blocks with the most inactive pages.

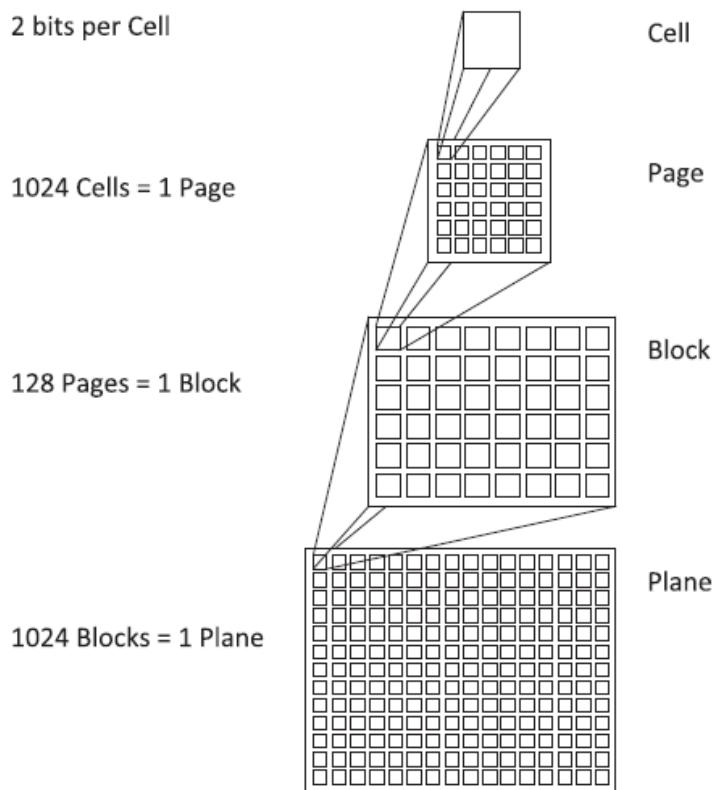


Figure 7. Hierarchy of the Flash Chip Architecture (Christopher King, 2011)

NAND flash uses tunnel injection for writing and tunnel release for erasing. NAND flash memory forms the core of the removable USB storage devices known as USB flash drives, as well as most memory card formats and solid-state drives available today.

Controller. The heart of the solid-state drive is the controller. The implementation of controller will have a huge impact on the performance of a solid-state drive. This controller manages all the aspects of the SSD and has a complex architecture. This controller is implemented as a stand on chip design and controls the NAND media. This controller is coupled with one or more embedded processor cores and consists of multiple hardware- accelerated functional blocks. Large SRAM (static RAM) for executing the SSD firmware is included in the ASIC, but often external DRAM (dynamic RAM) is used for caching both user data and internal SSD metadata (Michael Cornwell, 2012).

Host interface. This is a physical interface from the host system to SSD. Most commonly implemented host interfaces are SATA (Serial ATA) and SAS (serial attached SCSI). One of the new versions of storage interface for SSDs which is not used in HDDs is PCIe (Peripheral component Interconnect Express). This is used for the same purpose as I/O interface used in laptops and servers.

SSD controller functions.

Wear levelling. The flash wear-levelling is a technique used to help prolong the life of SSD or USB flash drives. Data can be written to the same flash drive a finite number of times. If we write the data repeatedly on the same drive more than its limit, it is possible that the drive could wear out at that location. So, flash drives use wear levelling technique to overcome this problem. Wear leveling works to distribute data evenly across each block of the flash drive. This process decreases the wear on the drive and increases the lifetime of the drive. This wear levelling is of two types:

Dynamic wear levelling: This type pools erased blocks and selects the block with the lowest erase count for the next write. It uses a map to link logical block addresses (LBAs) from the OS to the physical flash memory (Wear Levelling, n.d.). Each time the OS writes replacement data, the map is updated so the original physical block is marked as invalid data, and a new block is linked to that map entry. Each time a block of data is re-written to the flash memory, it is written to a new location (Wear Levelling, n.d.). However, flash memory blocks that never get replacement data would sustain no additional wear, thus the name comes only from the dynamic data being recycled. Such a device may last longer than one with no wear leveling, but there are blocks remaining as active even though the device is no longer operable. This method is most efficient for dynamic data because only the non-static portion of the NAND Flash array is wear-leveled. A system that implements dynamic wear leveling enables longer NAND Flash device life than a system that does not implement wear leveling.

Static wear levelling: The other type of wear leveling is called static wear leveling which also uses a map to link the LBA to physical memory addresses. Static wear leveling works the same as dynamic wear leveling except the static blocks that do not change are periodically moved so that these low usage cells are able to be used by other data (Wear Levelling, n.d.). This rotational effect enables an SSD to continue to operate until most of the blocks are near their end of life. This type of wear levelling increases the life of the device by utilizing all the good blocks to distribute the wear evenly. This even distribution of wear is done throughout the device by selecting the available block with least wear every time the program is executed. Blocks that contain static data with erase counts that begin to lag behind other blocks will be included in the

wear-leveling block pool, with the static data being moved to blocks with higher erase counts (Micron, 2008).

Table 2

Static vs. Dynamic Wear-Leveling Methods (Micron, 2008)

Wear Levelling Method	Advantages	Disadvantages
Static	Maximizes device life Most robust wear-leveling method Most efficient use of memory array	Requires more controller overhead Can slow WRITE operations Higher power consumption More complicated to implement than dynamic wear leveling
Dynamic	Improves device life over no wear leveling at all Easier to implement than static wear leveling No impact on device performance	May not optimize device life

Garbage collection. Garbage collection is a background process that allows a drive to mitigate the performance impact of the program/erase cycle by performing certain tasks in the background. Usually data in the memory flash drive is written in the units called pages. SSDs read and write the data at page level but can erase the data only at the block level. If the data in some pages of the block are no longer needed, only pages with good data in the block are read and rewritten into another previously erased empty block. Then the pages left by not moving the old data are available for new data.

The process of garbage collection is illustrated in the figure below. Column 1 shows the data is written in the Pages 1-4 in block A. After a while, the data is modified, and the Pages 1-4 are marked invalid and Pages 5-8 are written in the second column. Now the Block A is full, and the Space 1-4 is holding the invalid data which cannot be reclaimed until the whole block is erased.

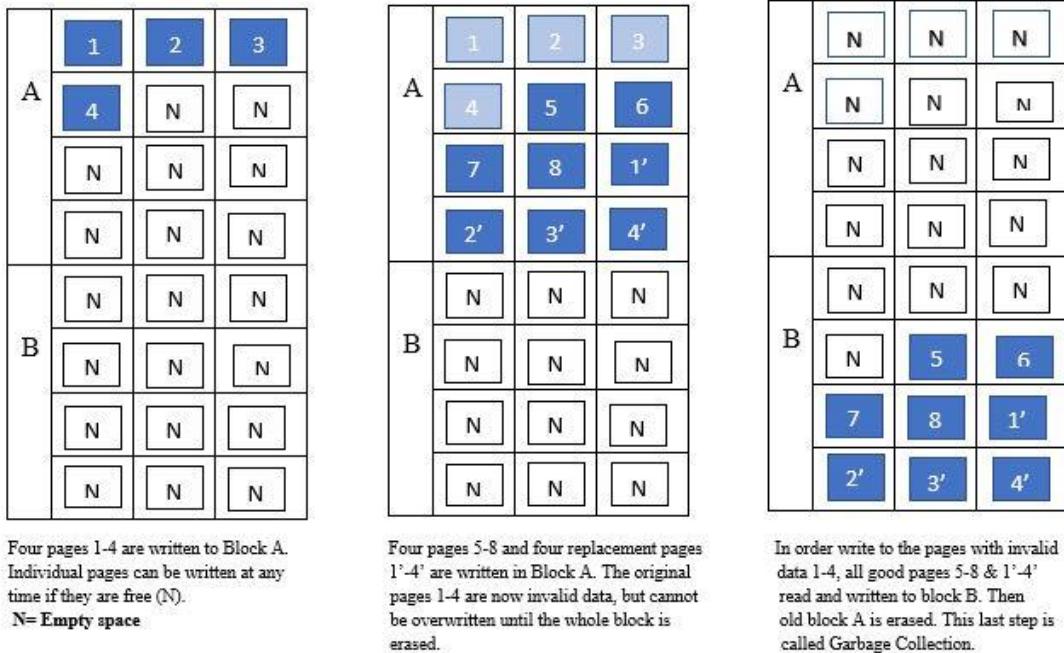


Figure 8. Garbage Collection Process

To make this process work, the valid data in the block A is moved to another block so that the original block can be used to start over. Column 3 shows the data from pages 1-4 and 5-8 are written to the new Block B so that Block A can be reclaimed for erasing it.

TRIM. TRIM 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. This TRIM command is designed to enable the operating system to notify the SSDs controller pages that contains stale data. This help the controller know not to relocate data stored on these pages during garbage collection, thereby lowering the number of writes to the flash memory (Ngo, 2013). TRIM helps lower the write amplification and increases the performance of the drive.

The TRIM command also erases the data which was already erased at the logical level, physically on the media. When a windows system is formatted, the saved files can no longer be referenced. If the format is done on an SSD, the affected memory areas will be available as

empty blocks for wear-levelling. These blocks are then subject to static wear levelling which results in write amplification. If the memory areas are used by the server again, the indispensable erasing of the flash memory cells can, contrary to what is otherwise the case, only take place immediately before a new write job (Fujitsu Technology Solutions, 2014). And writing on such flash memory cells is associated with higher response times. The way the TRIM command operates is considering the contents of discarded blocks as indeterminate (the “do no care” state) until the moment these blocks are physically erased by a separate background process, the garbage collector. In other words, the TRIM command does not erase the content of discarded blocks by itself. Instead, it adds them to a queue of pending blocks for being cleared by the garbage collector.

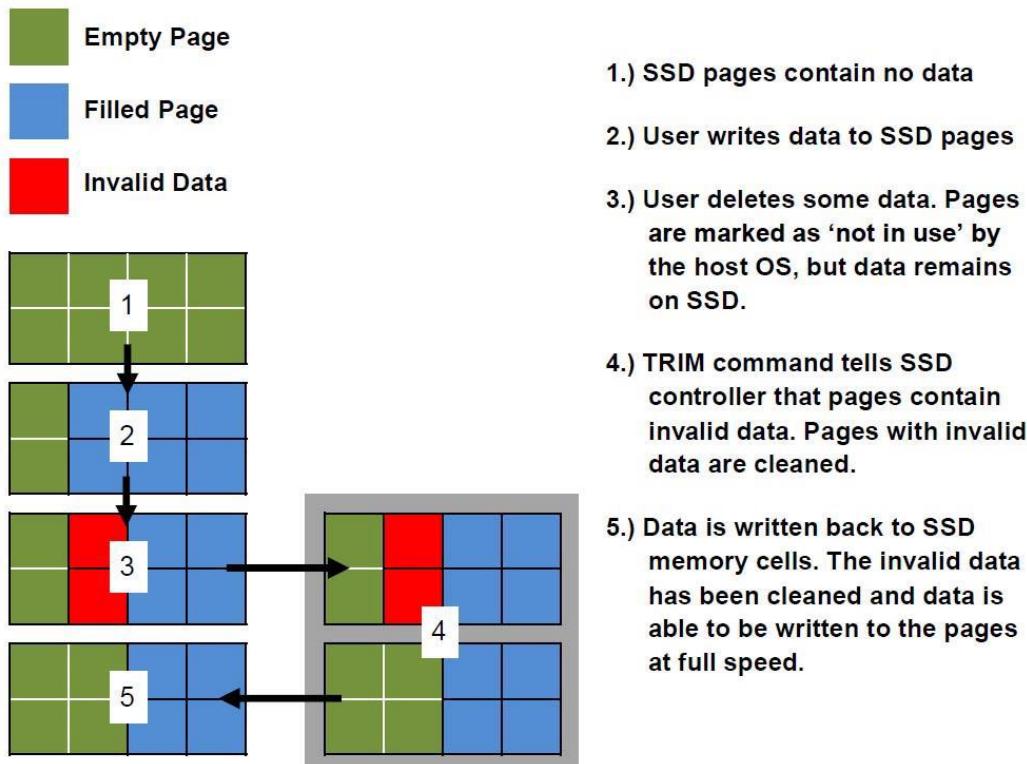


Figure 9. TRIM (Yuri Gubanov, 2014)

Literature Review Related to the Methodology

Functioning of a Drive with TRIM and Without TRIM

SSDs can read and write the data at page level which is usually 8KB. However, they also have a negative function which is they cannot erase the data at the page level and can erase only the entire block which are made up of hundreds of pages. The reason for this is that erasing a page's contents requires zapping that page with a not-insignificant amount of voltage, and the NAND-style layout of all modern SSDs makes it prohibitively difficult to isolate that voltage to only the pages that need erasing (Hutchinson, 2012).

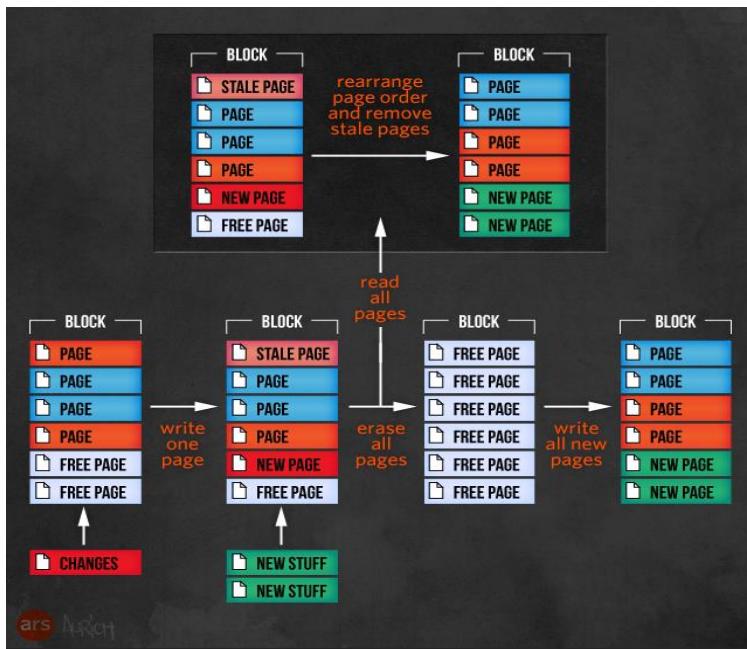


Figure 10. SSDs Can Only Be Erased One Whole Block at a Time (Hutchinson, 2012)

This is the only problem existing in the SSDs as the storage is full, it must erase the old blocks to create the space for new data. To prevent this, the SSDs have implemented new technology called as Garbage Collection to always keep a large reserve of empty blocks ready for writing. Garbage collection looks for blocks that contain a mix of good pages and stale pages

and then duplicates all the good pages and leaves behind only the stale pages in the old block.

Then it erases the whole old block and marks it ready for use.

When a file is deleted by the operating system, the file is do not delete but it simply marks it in some specific way as being overwritten by new data. Usually, a file system looks to the SSD as a series of writes and this is different from that of hard disk drive where there is a relation between file system clusters and disk sectors. In SSD, the correlation does not exist and the used pages must be tracked and picked up by the garbage collection. Pages containing deleted files look like valid pages, and they keep getting collected along with good pages (Hutchinson, 2012).

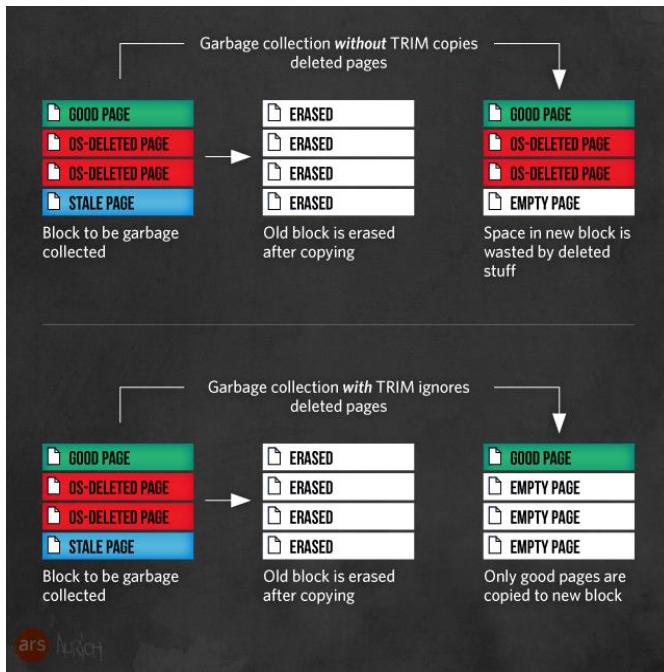


Figure 11. Garbage Collection with TRIM

Without TRIM, garbage collection does not know about deleted files and continues to move pages containing deleted data along with good pages, increasing write amplification.

TRIM tells the controller that it can stop collecting pages with deleted data so that they get left behind and erased with the rest of the block.

Entering TRIM. TRIM is an ATA command that the operating system can cause to be sent when it deletes a file. The TRIM command provides that bridge from the file level to the block level, giving the operating system a way to tell the SSD that it is deleting files and to mark those files' pages as stale. With TRIM, an SSD is no longer forced to save pages belonging to deleted files. TRIM does not obviate the need for garbage collection—it works with garbage collection to more properly mark pages as stale. And you do not need TRIM for garbage collection to work—but TRIM makes an SSD's garbage collection more efficient (Hutchinson, 2012).

TRIM Function in Windows Operating System

To use the TRIM command, the specifications required are, the operating system should support TRIM, i.e., it should be Windows 7 or higher version and the SSD needs to be compatible with TRIM. To check TRIM status on the OS, open the command prompt and type the following commands:

DisableDeleteNotify = 0: TRIM is already enabled and working in Windows,

DisableDeleteNotify = 1 : TRIM is not enabled

To enable SSD TRIM support in Windows, enter:

```
fsutil behavior set DisableDeleteNotify 0
```

Chapter III: Methodology

Introduction

In this chapter, we will be discussing on the procedure that is being used for research. We shall be discussing the key concepts like how the data is deleted from SSD, role of Garbage collection, TRIM command. We will also be discussing the data collection techniques, hardware and software requirements that are being used for our research.

Design of Study

This approach we are using is a quantitative study. To begin with, a windows operating system running on an SSD is acquired. The main motive of the experiment is to analyze the TRIM activity, so we try to acquire an operating which is Windows 7 or higher configuration. All the Windows 7 and above operating systems have an inbuilt TRIM command which can be modified by the user. So, we try to check the TRIM command and we will make sure that it is enabled on the operating system. The complete SSD is formatted and some files and documents are loaded into the system. Then, we use a tool called Forensic tool kit to create the image of the disk and search through the files using the keywords. The results obtained during the TRIM command is set to hypothesis for the study. Once the results are obtained, the trim command is disabled on the operating system by the administrator and the drive is formatted. The same files and documents are then loaded to the drive again and the same experiment is done while the TRIM command is disabled. The results obtained are then compared with the previous one and this will help us in analyzing the TRIM command status on the solid-state drives for resolving evidences in the forensic investigations.

Data Collection

This process involves a Laptop with solid-state drive which is HP Pavilion x360 Convertible Signature Edition, Intel(R) Core(TM) i5-6200 CPU @ 2.30GHz and 64-bit operating system. This is a Windows 10 operating system and a bulk of files, images, documents, media are created.

Firstly, a bulk of files and media are loaded on to the drive. Along with the random files, sample case files are also loaded onto the drive. Once the files are done uploading, an image is created using Forensic toolkit to analyze the evidence. The first instance is done by enabling the TRIM function. Once the results are obtained, the drive is cleared and the TRIM function is disabled and the same process is repeated. The results obtained are then compared with the previous results for the hypothesis of study.

Tools and Techniques

Forensic Toolkit or FTK is a computer forensic software made by the access data. It helps in scanning the drive for various information. It can be used for locating deleted emails, scanning the disk for text strings for using them as password dictionary for cracking encryption. This toolkit involves a standalone disk imaging program called FTK imager which is a simple but concise tool.

Hardware and Software Requirements

To perform this experiment, the main tool used is Forensic toolkit. Some of the other requirements are as follows:

Hardware Requirements:

- HP Pavilion x360 Convertible Signature Edition i5-6200 CPU @ 2.30GHz

- SSD VisionTek - Solid state drive - 120 GB - internal - 2.5-inch - SATA 6Gb/s
- HD Shredder

Software Requirements:

- Windows 10 operating system
- Forensic toolkit
- FTK Imager

Timeline

Start Date	End Date	Tasks	Duration
09/2/2017	09/24/2017	Referring to the articles on the topic	2 weeks
09/24/2017	10/10/2017	Gathering Information	2 weeks
10/10/2017	11/01/2017	Introduction and Literature review	3 weeks
11/01/2017	11/08/2017	Completing Documentation for Proposal	1 week
11/08/2017	11/29/2017	Gathering files for the implementation	3 weeks
11/29/2017	12/15/2017	Creating an Image File	2 weeks
12/15/2017	12/30/2017	Analyzing the images on SSD	2 weeks
12/30/2017	01/21/2018	Images of SSD without TRIM	3 weeks
01/21/2017	02/05/2018	Comparing the results	2 weeks
02/05/2018	02/20/2018	Analysis on the results	2 weeks
02/20/2018	03/05/2018	Report on Implementation	2 weeks
03/05/2018	03/15/2018	Complete report for defense	1 week

Chapter IV: Data Presentation and Analysis

Introduction

In this chapter, we will discuss on analyzing how trim function is enabled and the effectiveness of how it works. During this process, we will compare hard disk drive and solid-state drive and analyze the results obtained from the drives. We will discuss on how the data is gathered and erased from the drives by altering the trim command. Later, we will compare the results obtained by performing forensic analysis using forensic toolkit.

Data Presentation

During this process, the data collected contains images, pdf files, documents, and various other files. The key source of evidence contains various folders which intern has sub-directories and folders. Different files are placed in all the drives for performing the forensic investigation.

Installation of FTK Imager

In-order to build an evidence image out of the files, we require FTK imager and below are the steps to download the FTK Imager:

1. Open <https://accessdata.com/product-download/ftk-imager-version-3.4.3> website to download FTK imager.
2. The FTK Imager webpage is as follows:

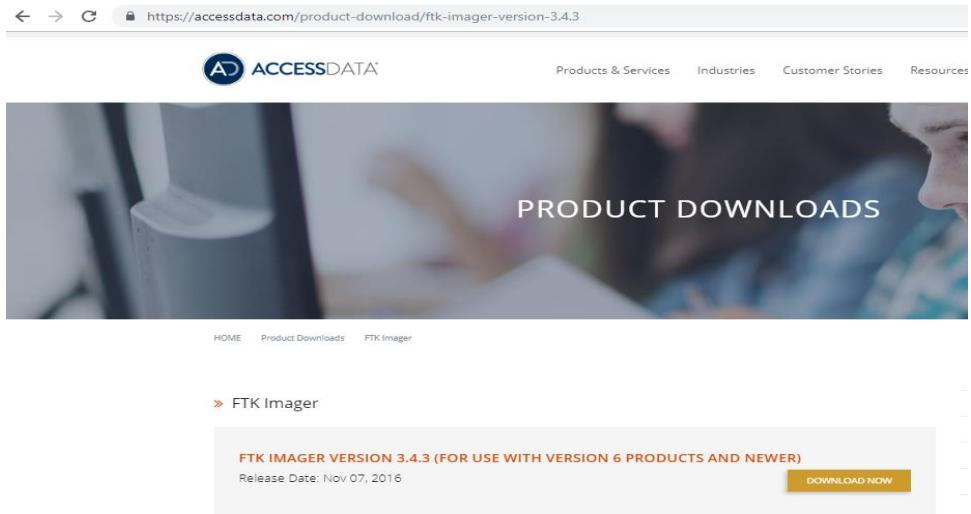


Figure 12. Installation Page for FTK Imager

3. The next step would be downloading the imager which redirects us to a new page where we need to give in all the details as follows:

Download FTK Imager 3.4.3

First Name

Last Name

Email

Phone

Country

Organization

Job Title

Organization Type

My organization is currently using FTK

Opt In Yes*

Submit

Figure 13. Details Page to Download the FTK Imager

4. We then fill in all the details required to download and click on submit which would redirect us to the following webpage:



[Download FTK Imager 3.4.3](#)

Thank you for downloading FTK Imager. The link to the free download has been sent to the email address you've provided. Please allow up to 15 minutes for the email to arrive and be sure to check your spam folder. If you do not receive the email, please send an email to webmaster@accessdata.com.

If you have opted out of receiving email communications from AccessData, you will not receive the confirmation email with the download link for FTK Imager. If you would like to opt back in, visit our [email preferences center](#).

Figure 14. Download Confirmation Page

5. We then receive a confirmation email from Access Data as follows:

Thank you for downloading FTK® Imager 3.4.3. If you have any questions or are interested in getting the full version of FTK, please email us at sales@accessdata.com.

[Download FTK Imager 3.4.3](#)

For instructions on how to use, view the [eForensics Magazine "FTK Imager Step by Step"](#) issue for step by step instructions or the [FTK User Guide](#).

After you create an image of the data with FTK Imager, you can then use AccessData® Forensic Toolkit® (FTK®) to perform a thorough forensic examination and create a report of your findings. For information about FTK, which is recognized around the world as the standard in computer forensic software, visit the [FTK web page](#).

ACCESSDATA 588 West 400 South Suite 350
Lindon, UT 84042 ☎ 801.377.5410
✉ [Contact Us](#)

[unsubscribe from this list](#) | [update subscription preferences](#)

Figure 15. Confirmation Email from Access Data

6. Click on Download FTK imager and we see the installation process as follows:

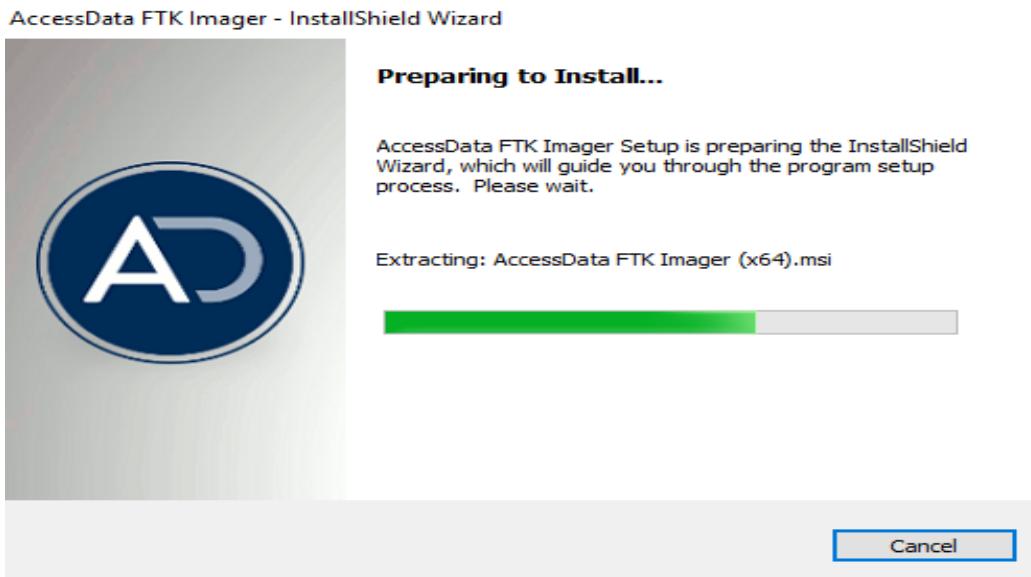


Figure 16. InstallShield Wizard for FTK Imager

7. As a part of the installation process we see the next steps as follows:



Figure 17. First Step of Installation Wizard

8. We click on next and accept the user agreement as follows:

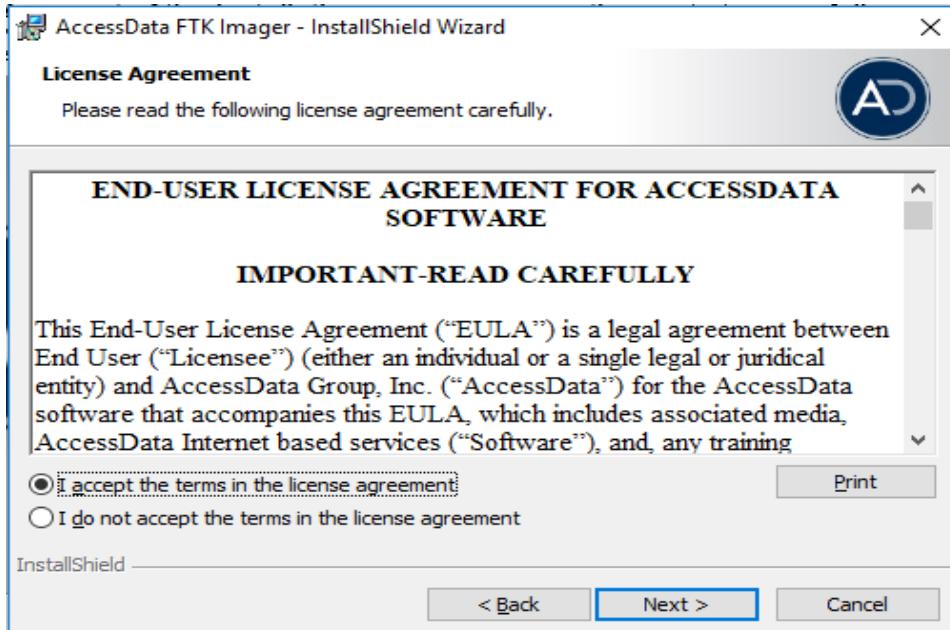


Figure 18. User License Agreement for Access Data Software

9. Select the directory where we need to install FTK imager as follows:

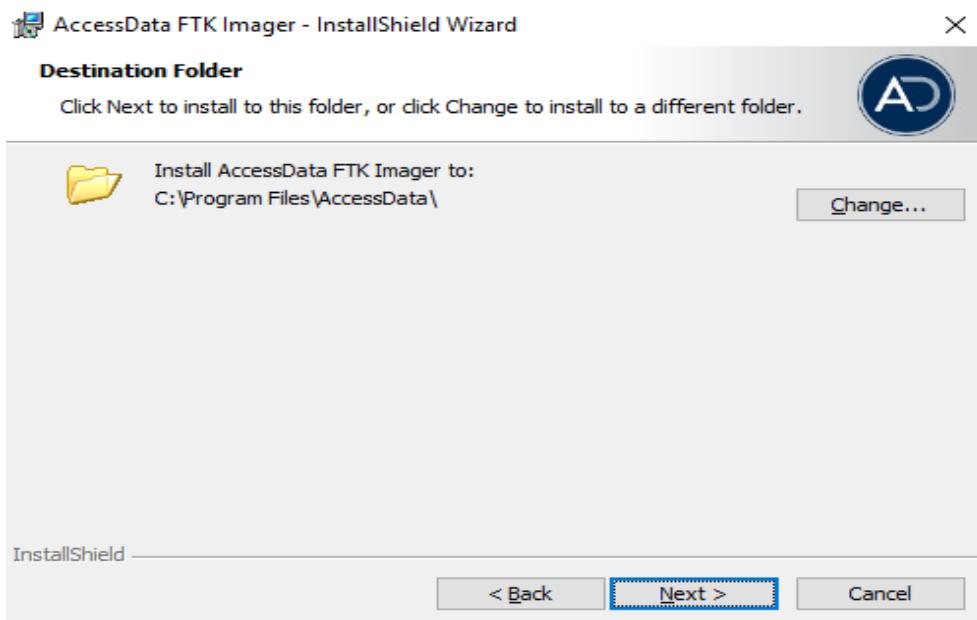


Figure 19. Selecting the Destination Folder for Installation

10. Next step would be installation process for FTK Imager as follows:

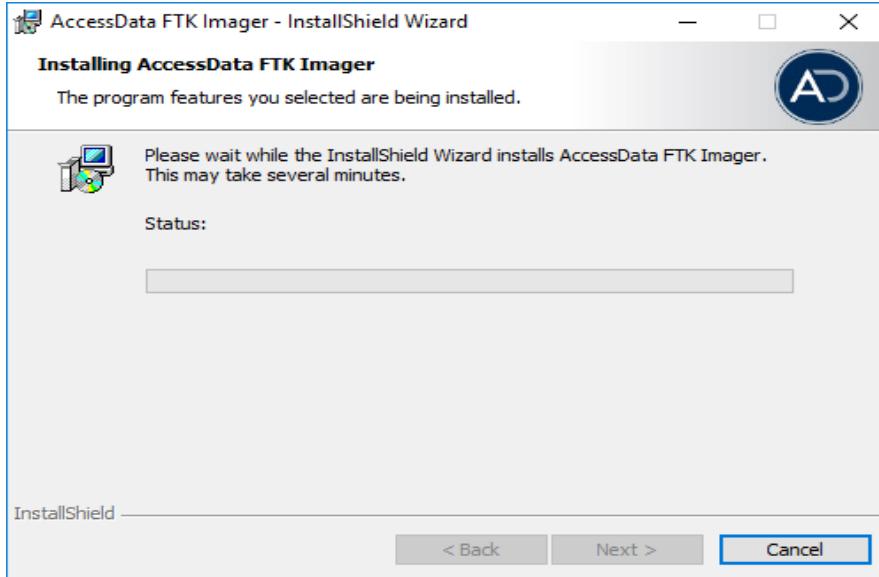


Figure 20. Selecting the Destination Folder for Installation

11. We then launch the FTK imager after installation and below is the preview:

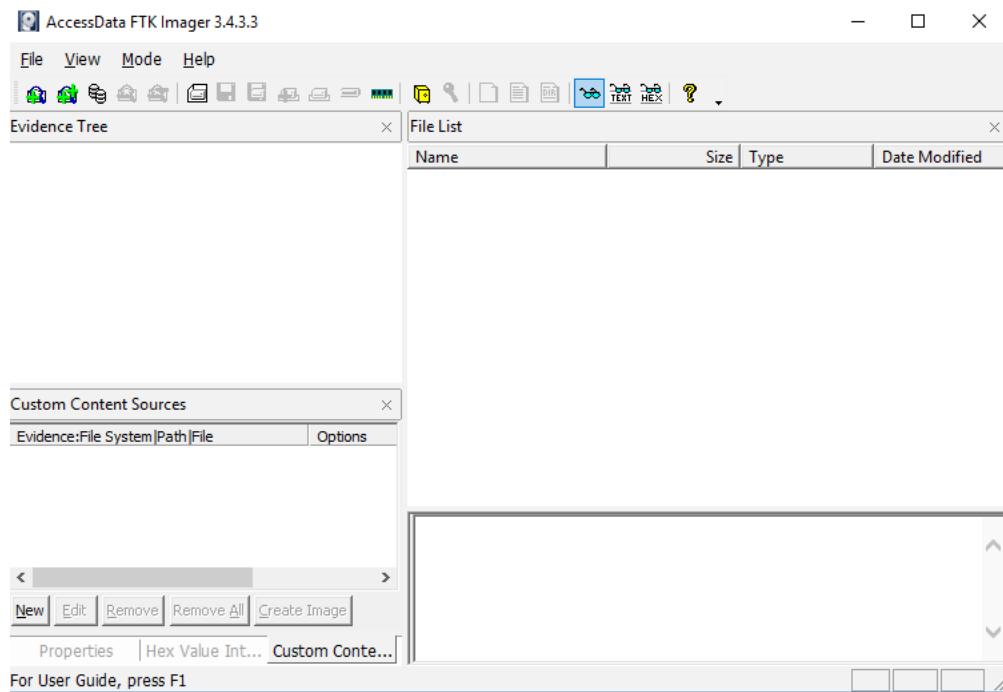


Figure 21. User Interface for FTK Imager

Forensic Toolkit (FTK)

FTK is used to filter, analyze, investigate, and report on acquired evidence. It “provides users with the ability to perform complete and thorough computer forensic examinations. FTK features powerful file filtering and search functionality. FTK customized filters allow you to sort through thousands of files so you can quickly find the evidence you need.

Steps for downloading Forensic Toolkit:

1. The first step of the installation process would be visiting the Access Data website and selecting the appropriate version to download which is shown below:

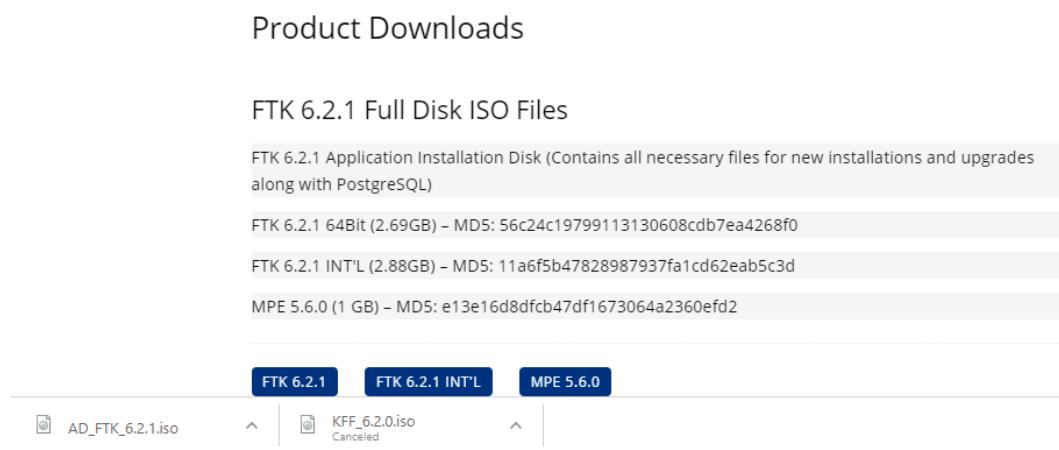


Figure 22. Access Data Website Which Shows the Forensic Toolkit Version to Download

2. Click the Forensic toolkit autorun which would open the following installer window:



Figure 23. Forensic Toolkit Installer Window

3. Below is the Startup page for Forensic Toolkit Installation wizard:



Figure 24. Forensic Toolkit InstallShield Wizard

4. Once we click on next button, it redirects us to the license agreement page as follows:



Figure 25: License Agreement Window for Forensic Toolkit

5. The next step of installation process would be selecting the advance setup type which includes Forensic Toolkit Installer. The default option would only install POST GRE SQL.

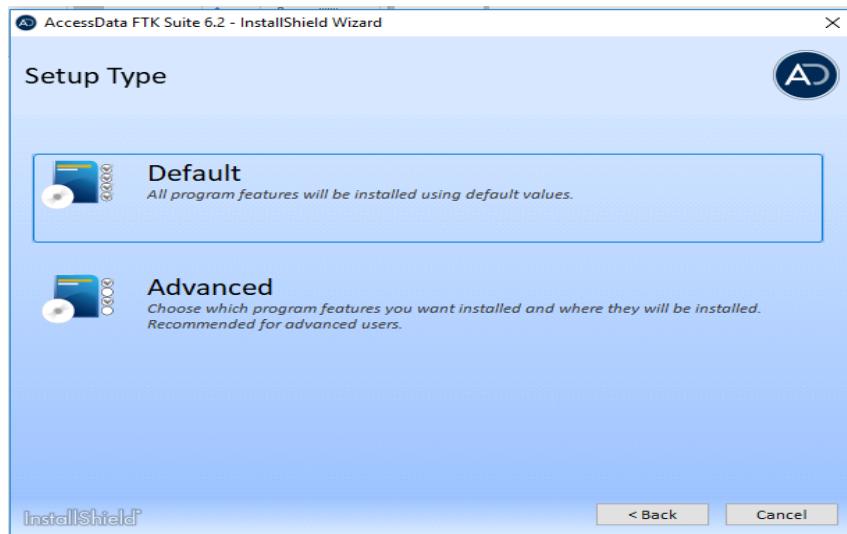


Figure 26. Setup Type Window for Installing Toolkit

6. Below is the window which displays the installation progress:

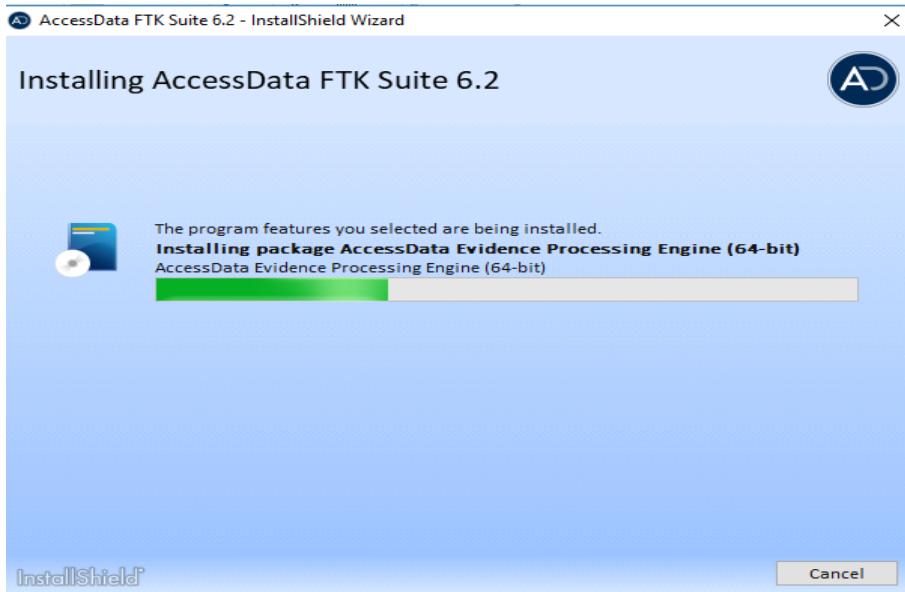


Figure 27. Progress of Installation for FTK Suite

7. Once the installation process is completed, the below window appears confirming that the installation process is complete, and the toolkit is ready to use:

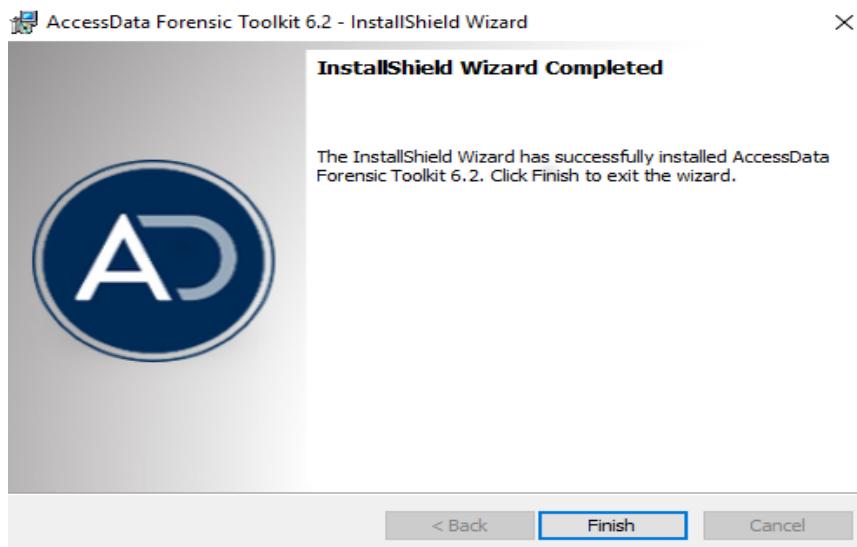


Figure 28. Completion of Installation for FTK Suite

Key Files of Interest

In this stage we will gather the data which comprises of various files and folders.

Below is the image which shows External Hard Disk connected to the laptop.

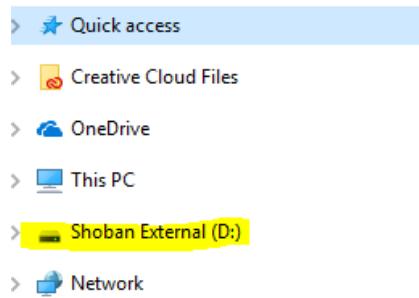


Figure 29. External Hard Disk Drive Connected to the Laptop

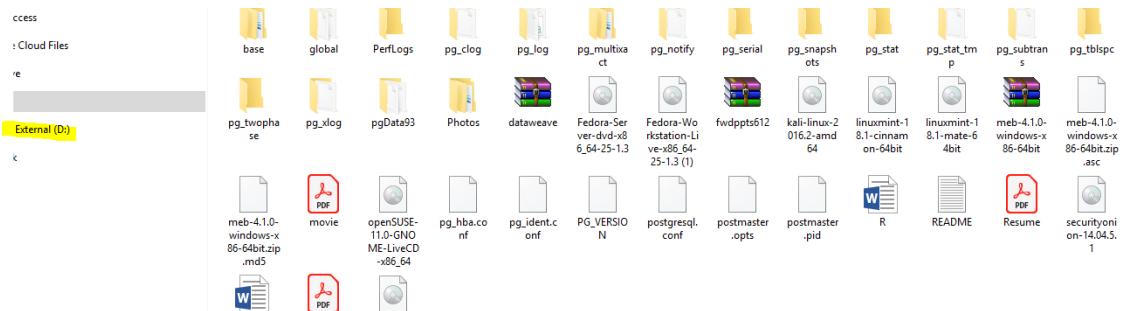


Figure 30. Folders and Files in the Hard Disk Drive

Solid State Drive

Contents of Solid-state drive. The image below shows the solid-state drive connected externally using ESATA port to identify the data in the internal SSD.

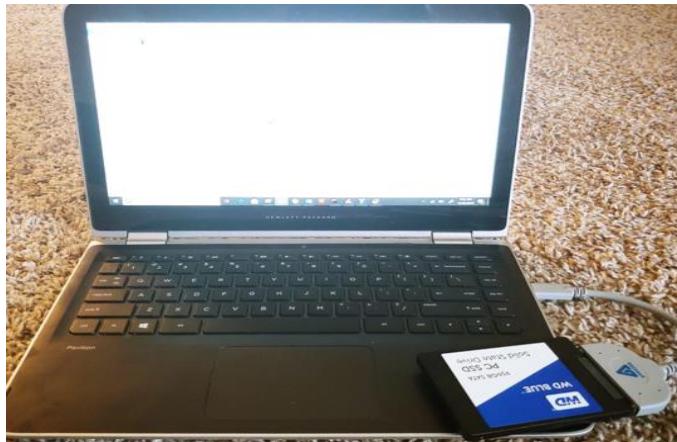


Figure 31. Internal SSD Connected Externally to a System Using ESATA Port

The files and folders are loaded into the solid-state drive. Below image displays the free space and the allocated space in the solid-state drive:

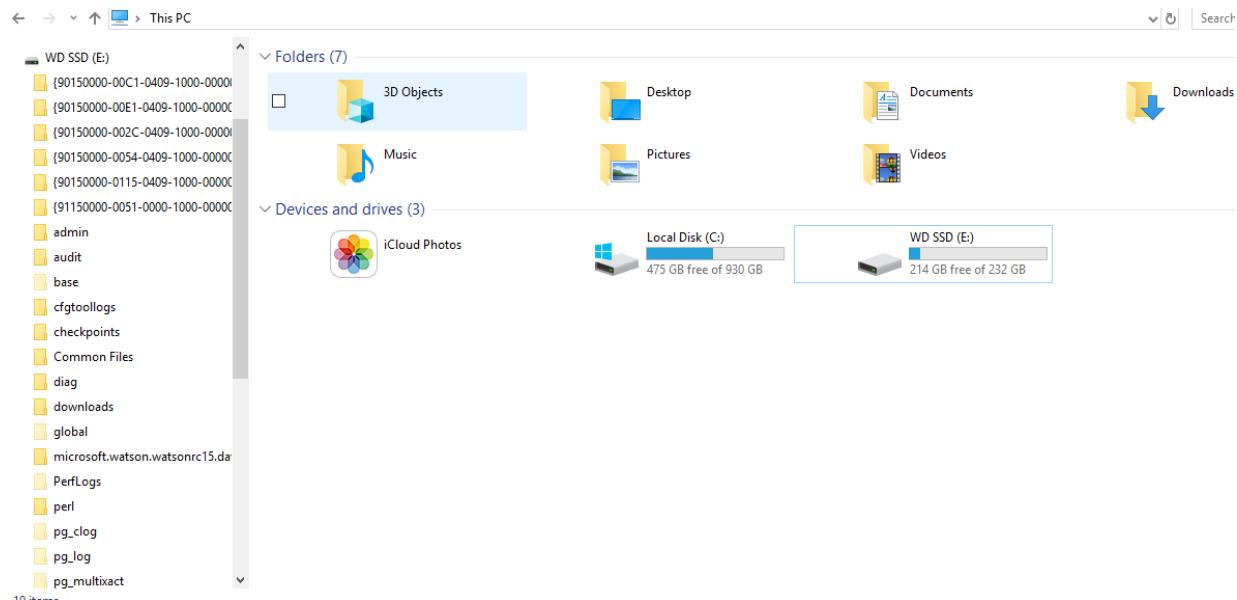


Figure 32. Displaying Disk Allocated Space and Used Space for Solid-State Drive

The files and folders are loaded into the solid-state drive and the below image shows the data in the drive:

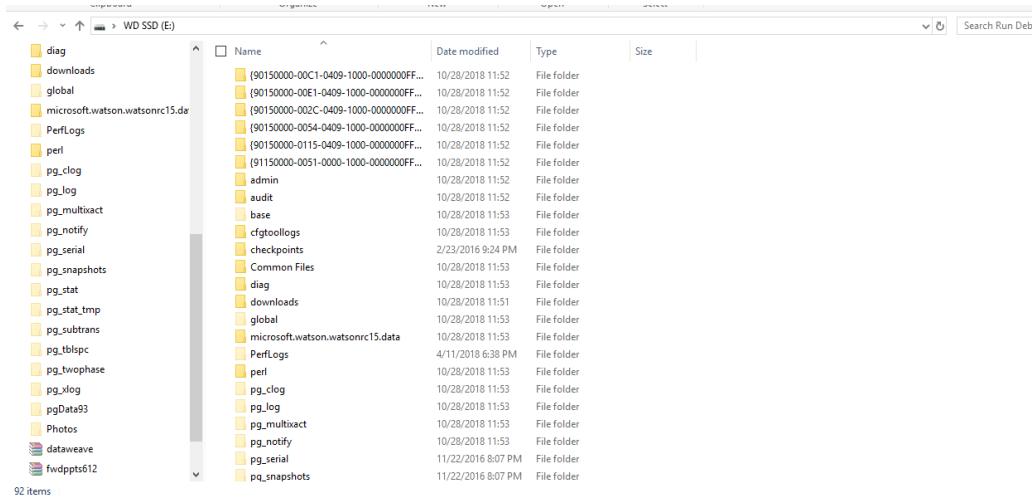


Figure 33. File and Folders in the Solid-State Drive

Once the data is loaded into the solid-state drive, the memory in the drive is allocated with some space for the data which is shown as below:

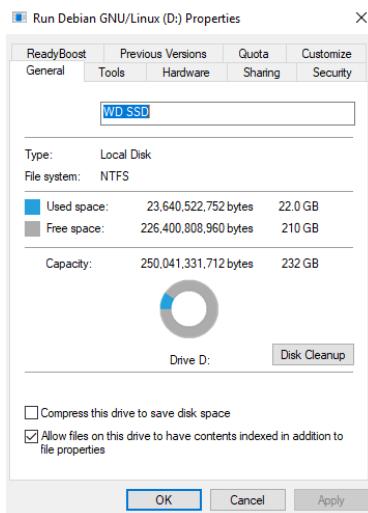


Figure 34. Image Displaying the Free and Allocated Space in the Solid-State Drive

Data Analysis

Hard Disk Drive Image

The Trim is set to the disabled state and the next step would be creating an image out of the hard disk drive. To perform this operation, we use Forensic toolkit imager which has been installed on the system.

Forensic Toolkit, or FTK, is a computer forensics software made by AccessData. It scans a hard drive looking for various information. It can, for example, locate deleted emails and scan a disk and create a image out the drive to perform forensic analysis.

Creating an image out of a drive, would involve several steps and the first step would be opening the FTK imager.

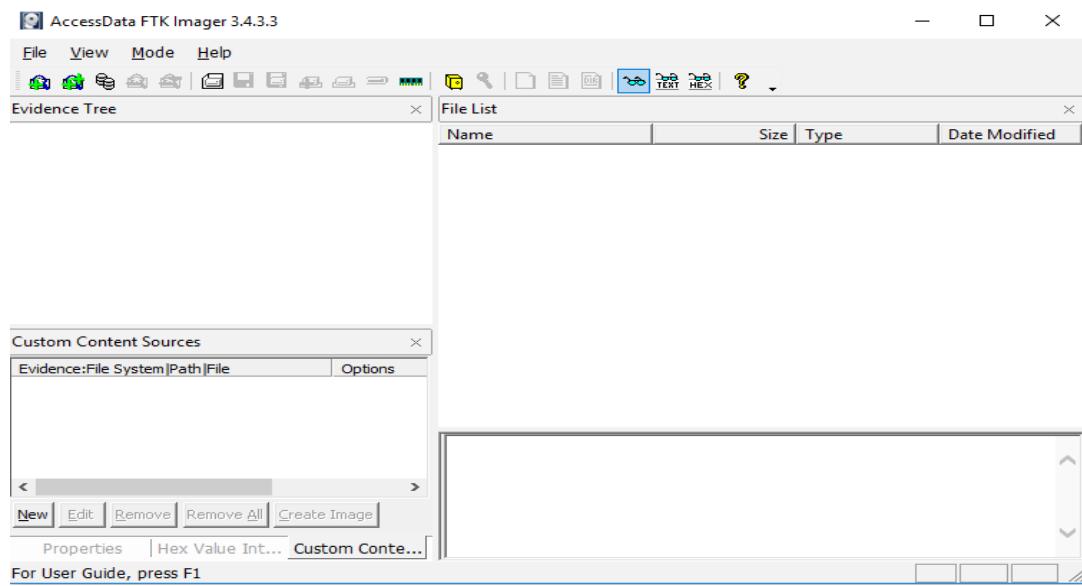


Figure 35. Window Displaying the FTK Imager

We then click on file and go to create disk image.

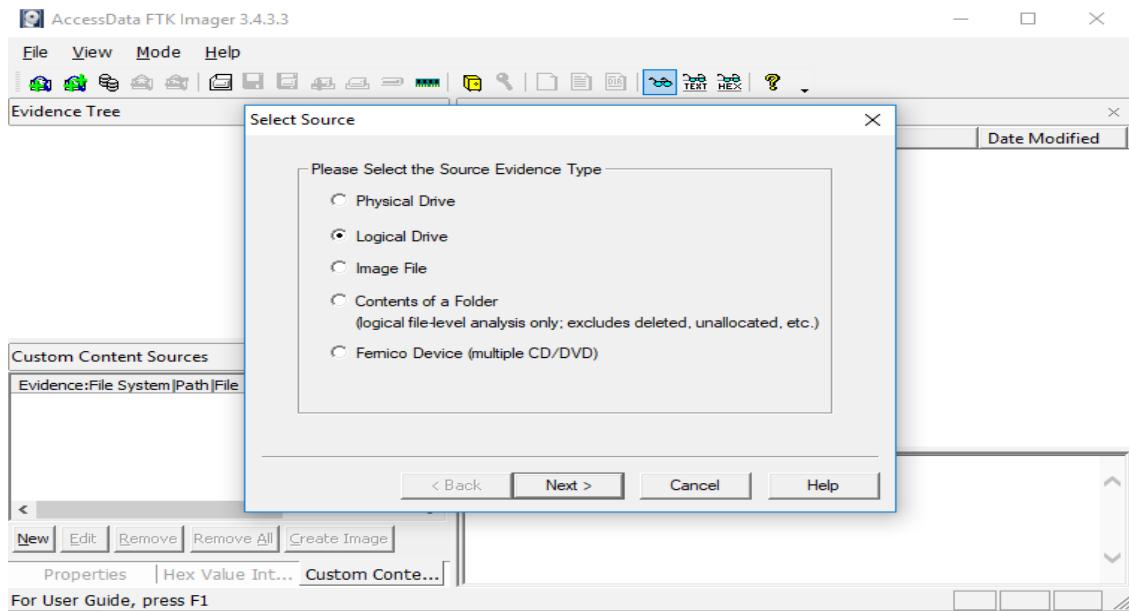


Figure 36. Loading the Logical Drive to Create an Image

The next step in this process is to select the appropriate drive to create the image.

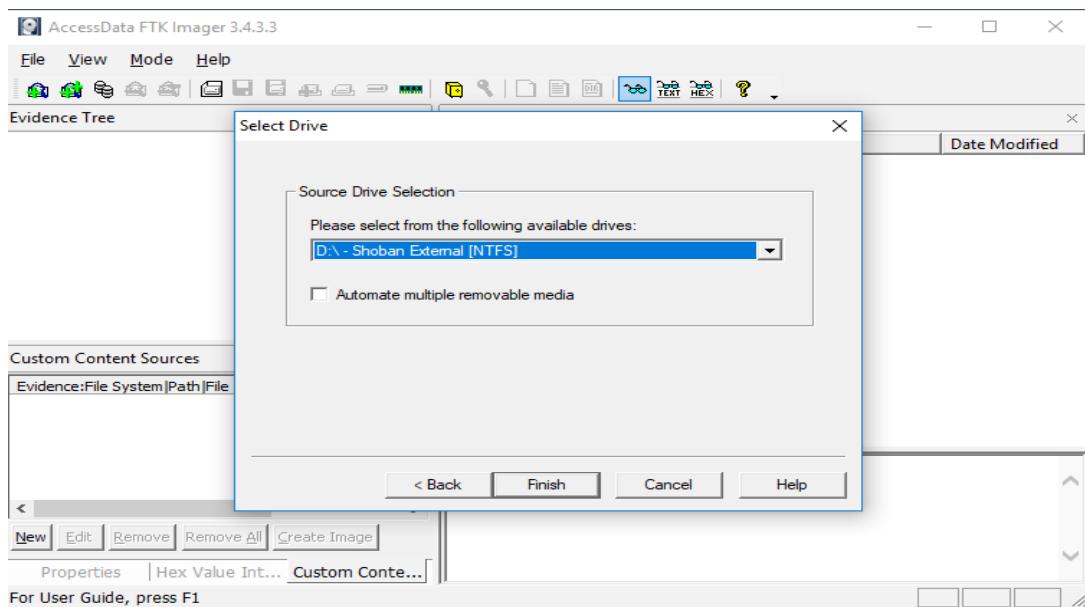


Figure 37. Selecting the Appropriate Drive to Create the Image

Click on the Add button to add the image destination so that the image is stored at a given location.

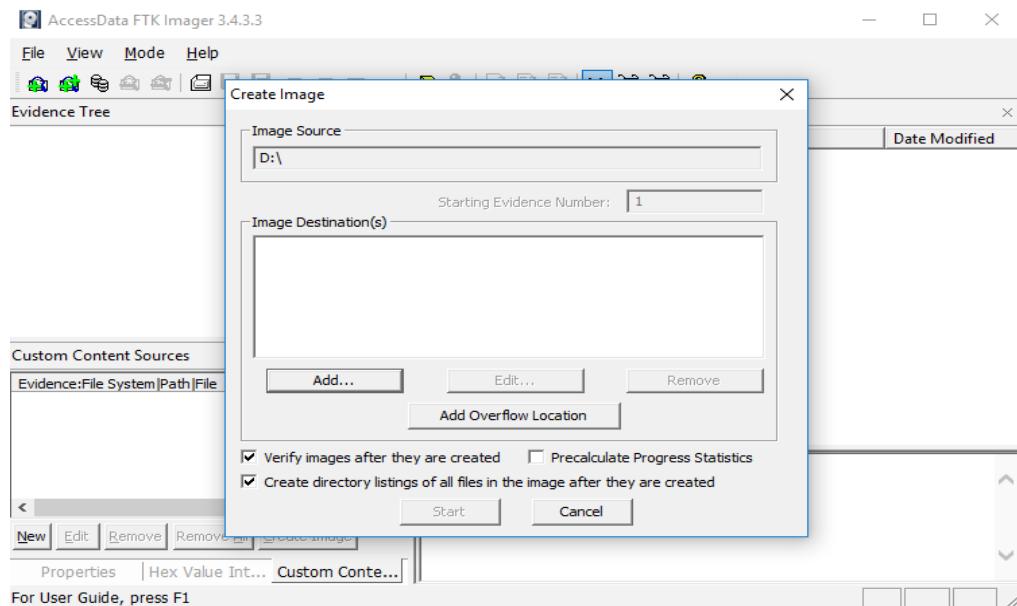


Figure 38. Adding a Destination Location to Save the Image

After selecting the destination location, we have to select the destination image type.

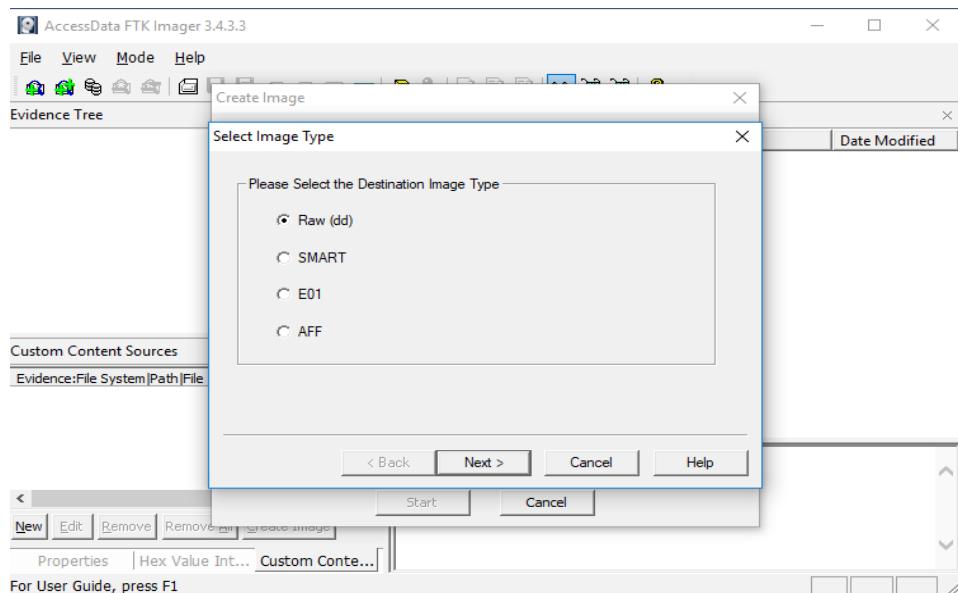


Figure 39. Selecting the Destination Image Type

Provide the evidence item information which is shown as below:

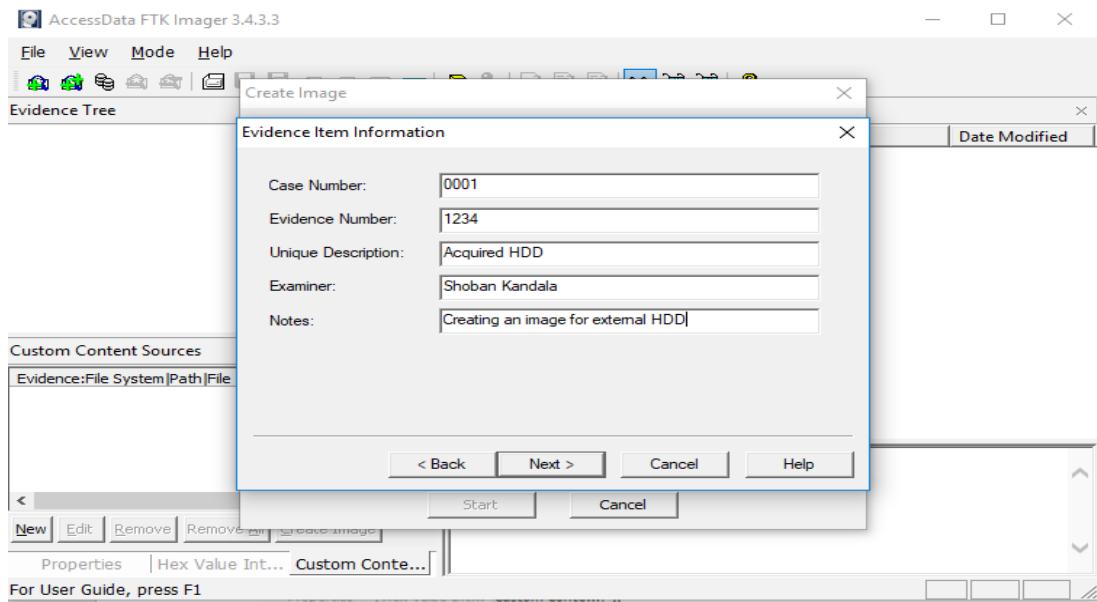


Figure 40. Evidence Item Information

The evidence item is filled out appropriately and once, we click on next button, the imager would us to enter the image file name so that the image that is being created will have a specific name.

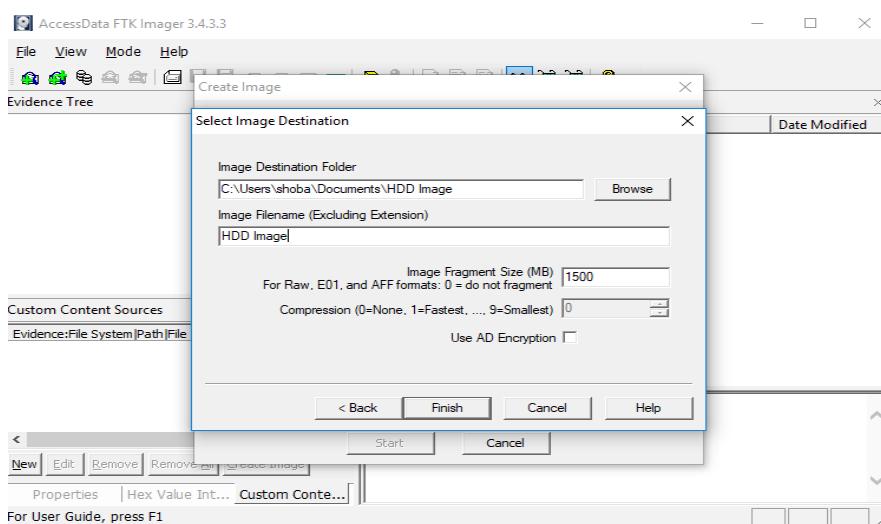


Figure 41. Giving a Specific Image File Name

Click on finish button to start the image creation process.

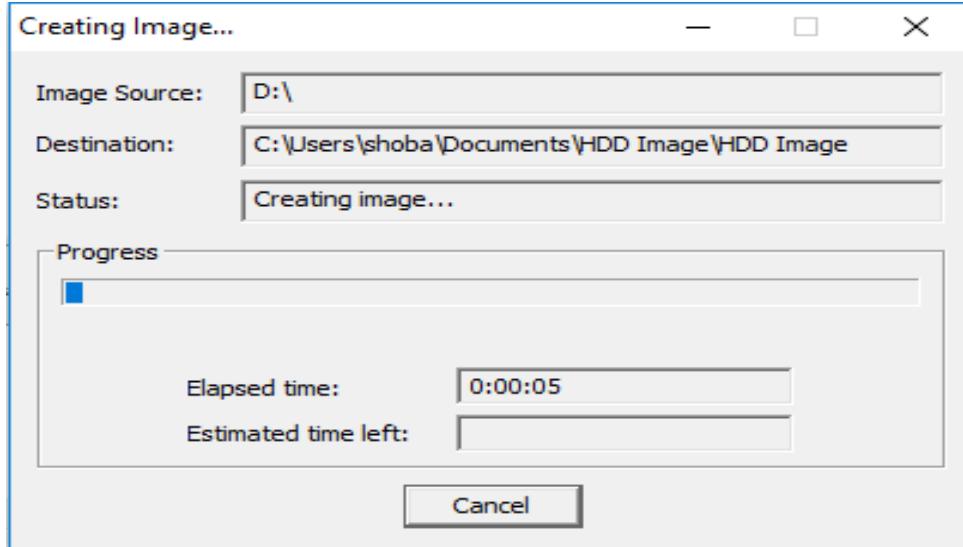


Figure 42. Window Displaying the Image Creation in Progress

Once the image creation is finished, the imager would display the finished window.

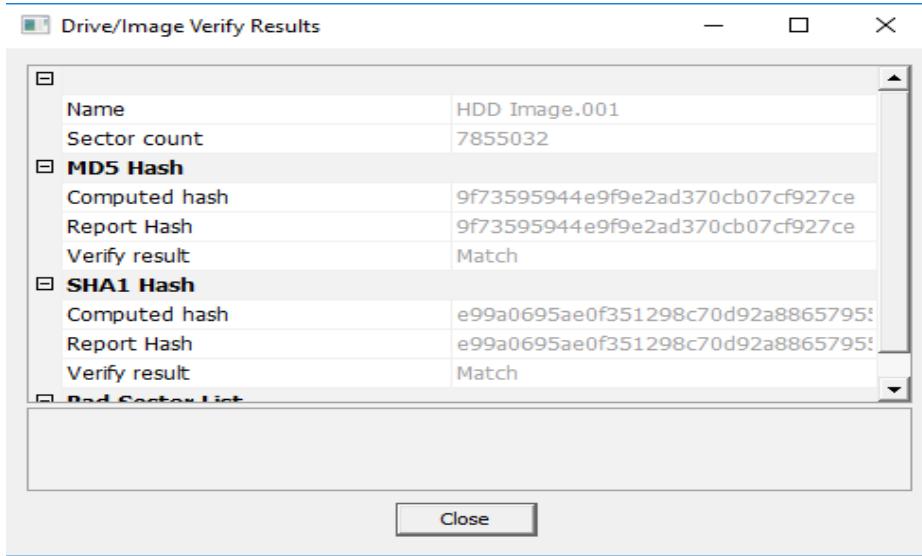


Figure 43. Window Displaying the Image Creation Completion

Now the image is completely created, and the next step will be mounting the image on the Forensic toolkit to perform the analysis. We open the Forensic toolkit and fill in the details to start the process.

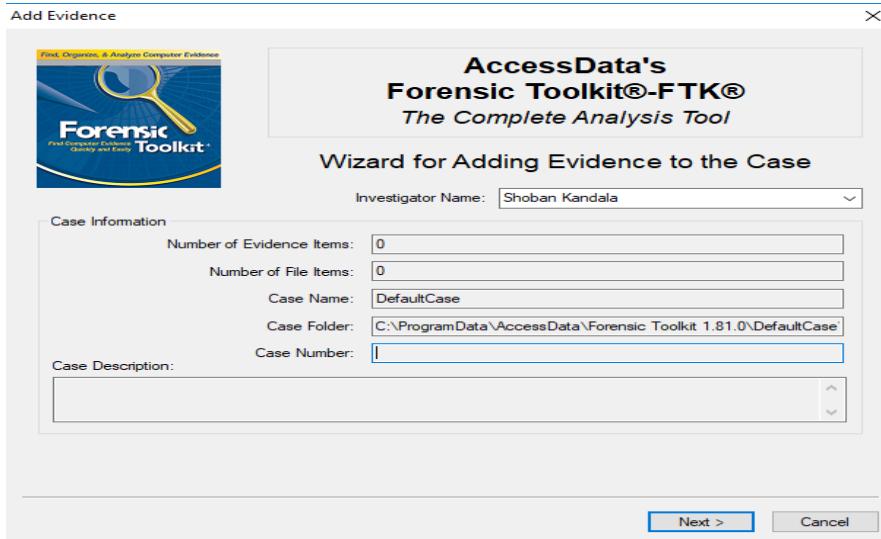


Figure 44. Access Data's Forensic Toolkit Wizard for Adding Evidence to the Case

In order to perform the mounting of the image, we must select the file types to be added by checking the appropriate check boxes as below:

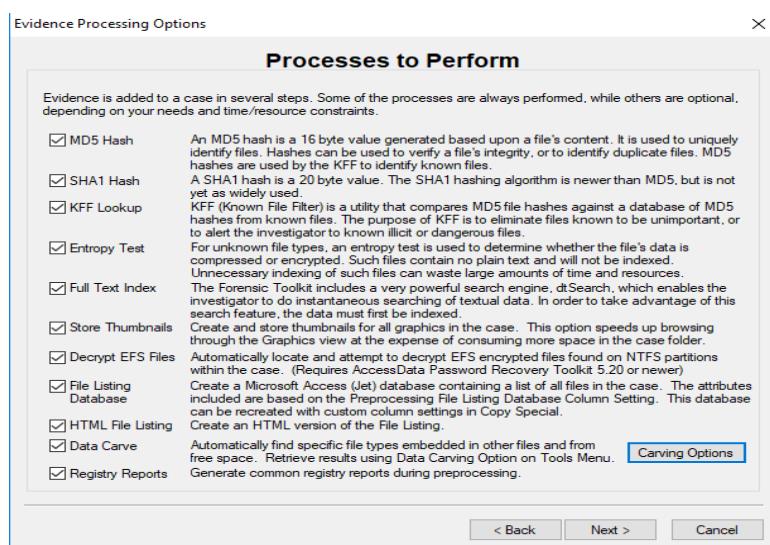


Figure 45. File Type Selection to Perform the Image Mounting

Select the acquired image to add the case.

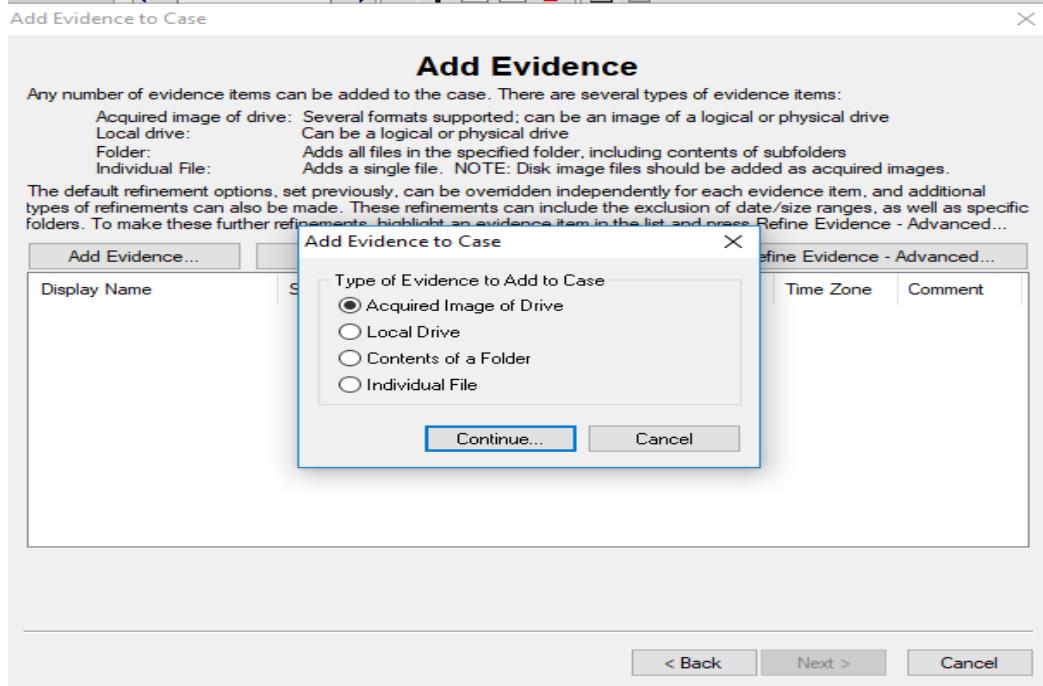


Figure 46. Adding Acquired Image as Evidence

Clicking on continue would redirect to the local destination and we have to select the image saved destination and select all the acquired imaged to mount.

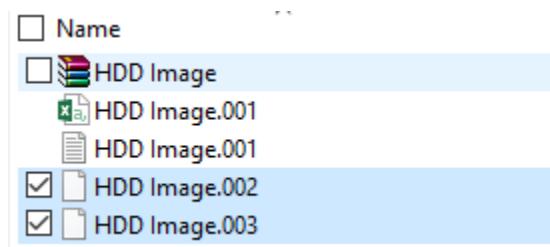


Figure 47. Adding Acquired Images from the Local Destination

After selecting all the images, we must provide the evidence information as shown below:

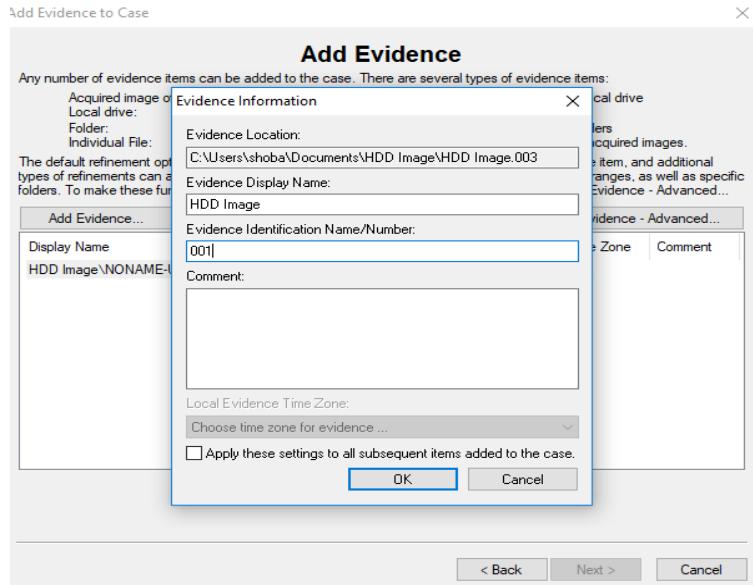


Figure 48. Providing the Evidence Information for the Image

The window below shows the complete setup after adding the images to the toolkit and we then click on finish to start the mounting images.

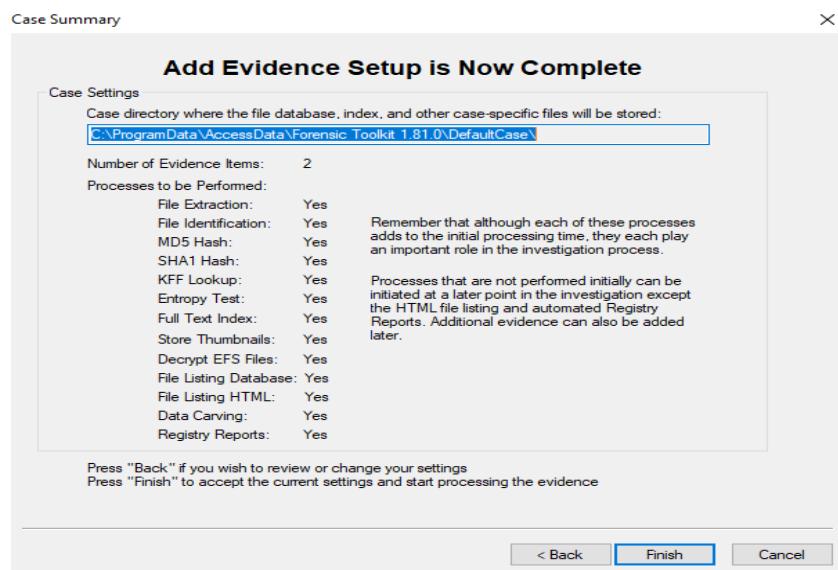


Figure 49. Setup Completion Window

The forensic toolkit will start processing the images that are added as the evidence.

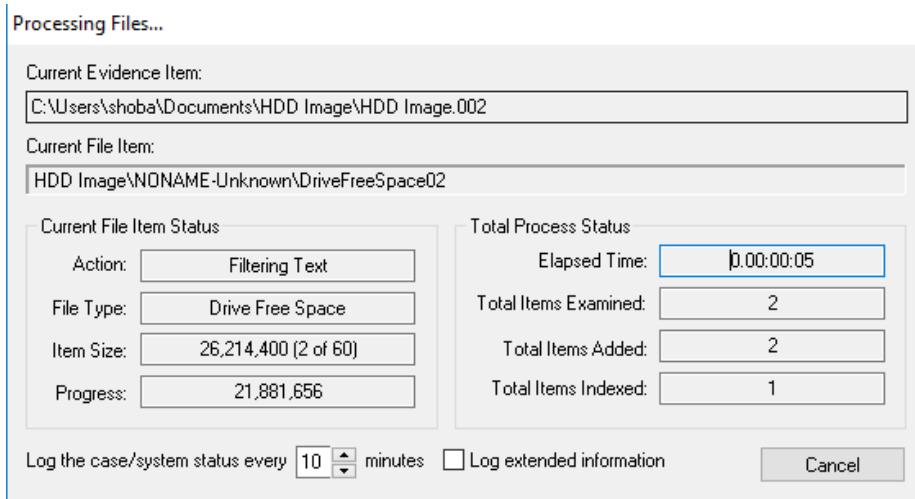


Figure 50. Forensic Toolkit Processing the Files

The image below shows the total files added to the forensic toolkit which are retrieved from the images.

Evidence items: 15

Total number of files and folders on the images: 915

The screenshot shows the 'Evidence Items' view in EnCase Forensic. The interface includes a navigation bar with tabs for Overview, Explore, Graphics, E-Mail, Search, and Bookmark. Below the navigation bar is a table titled 'Evidence Items' with columns for 'File Status' and 'File Category'. The table lists various file types and their counts. A large central pane displays a list of files with columns for File Name, Full Path, Recycle Bin..., Ext, File Type, Category, Subject, Cr Date, Mod Date, Acc Date, L-Size, P-Size, and Chi. The list includes numerous entries for 'HDD Image\NONNAME\Unknown\DriveFreeSpace' files, each with a unique name and timestamp. At the bottom, there are status bars for '9451 listed', '0 Checked Total', and '0 Highlighted'.

Figure 51. Files Retrieved from the Mounted Images

Performing the Analysis by Erasing the Data from Hard Disk Drive

Analysis on Hard Disk Drive

To perform this analysis, we erase the data completely from the hard disk drive. Now the drive is completely empty as shown below:

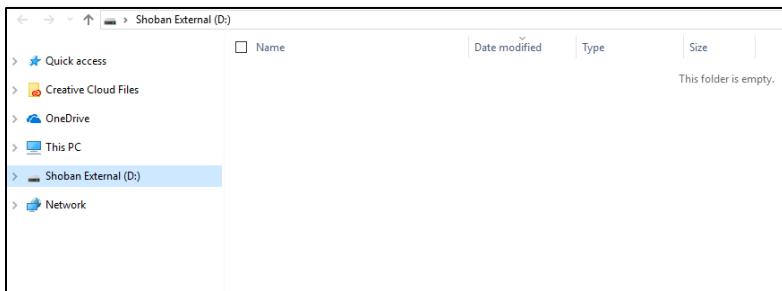


Figure 52. Erased Hard Disk Drive

Once the data is erased from the hard disk drive, we then perform the analysis on the data in the drive. The first step in this process is to change the trim command and perform the data analysis. We check for the TRIM command status and change disable it to perform the first step of analysis.

To check the TRIM status, we should open the command prompt as an administrator and check for the TRIM status with *fsutil behavior query disabledeletenotify*.

```
Windows PowerShell
Copyright (c) Microsoft Corporation. All rights reserved.

C:\Users\shoba>fsutil behavior query disabledeletenotify
NTFS DisableDeleteNotify = 0 (Disabled)
ReFS DisableDeleteNotify = 0 (Disabled)

C:\Users\shoba>
C:\Users\shoba>
```

Figure 53. Command Prompt Running as an Administrator and Query to Show the Status of TRIM on the System

We must make sure that the TRIM is completely disabled. To set the TRIM as disabled, we use *fsutil behavior set disabledeletenotify 0*



```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.17134.345]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>fsutil behavior set disabledeletenotify 0
NTFS DisableDeleteNotify = 0 (Disabled)

C:\WINDOWS\system32>
C:\WINDOWS\system32>
```

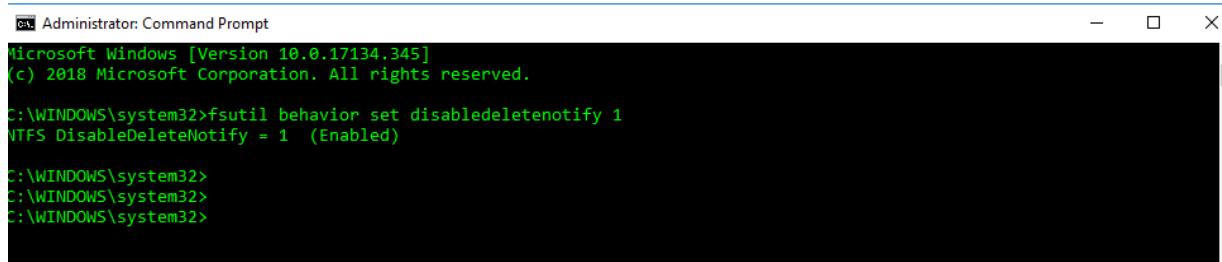
Figure 54. TRIM Command Set to the Disabled Status

The images that are created by FTK imager is mounted on the Forensic toolkit and all the files are retrieved by the toolkit. Now we disable the TRIM status and erase the data from the hard disk and perform the analysis.

To disable the trim on the system, we run the command prompt as administrator and use the following command:

fsutil behavior set disabledeletenotify 1

The image below shows the command prompt with the trim status enabled.



```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.17134.345]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>fsutil behavior set disabledeletenotify 1
NTFS DisableDeleteNotify = 1 (Enabled)

C:\WINDOWS\system32>
C:\WINDOWS\system32>
C:\WINDOWS\system32>
```

Figure 55. Command Prompt with TRIM Status Enabled

The results obtained after retrieving the data from hard disk drive after the trim is enabled is shown as below:

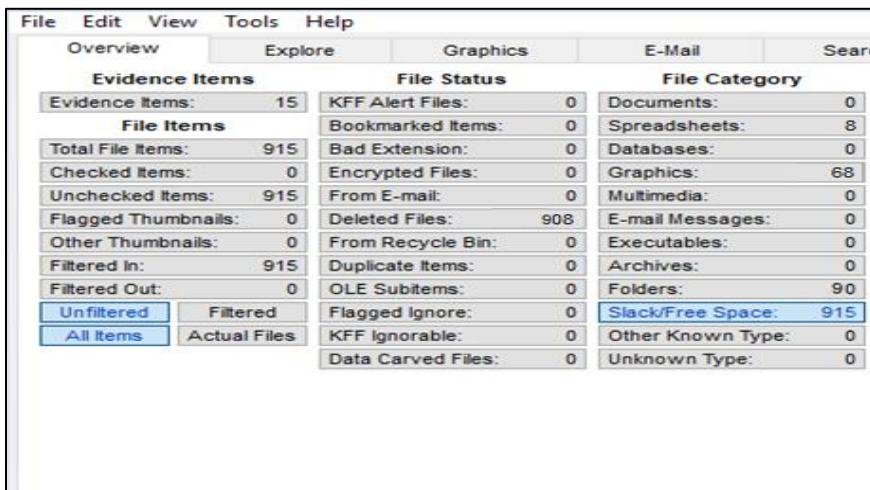


Figure 56. Image Showing the Results for Hard Disk Drive

Analysis on Solid-State Drive

To perform the analysis on solid state drive, we must change the trim status to disable state and then carry out the analysis. After the trim status is disabled, we then create an image for then files and folders on solid state drive.

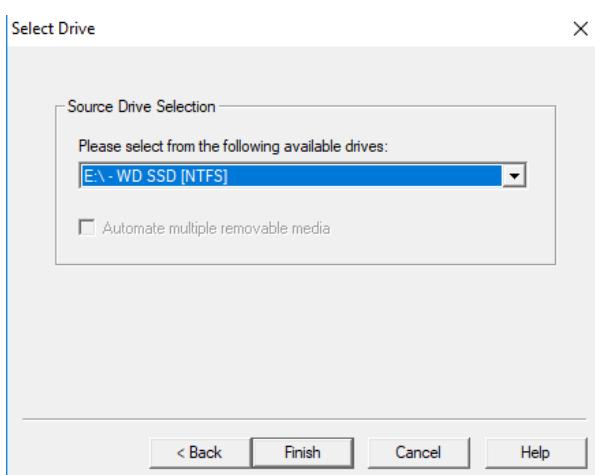


Figure 57. Mounting the Solid-State Drive to Perform Analysis

We then give the details of the evidence information which is shown as below:

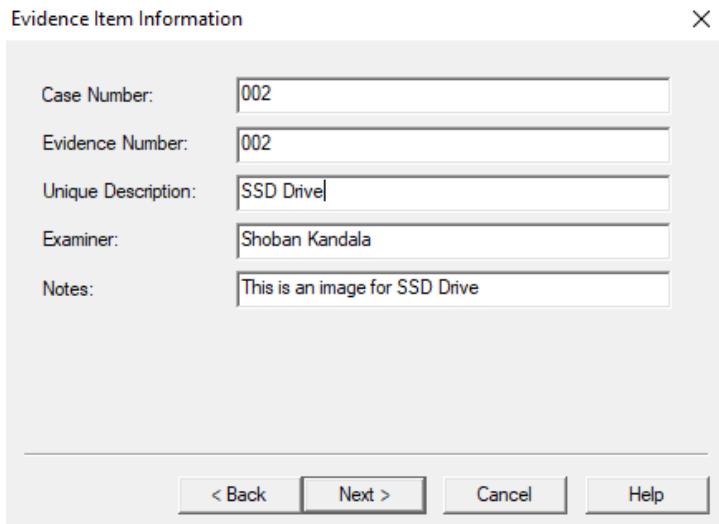


Figure 58. Evidence Item Information

After entering the source, we have to select the image destination and load the image.

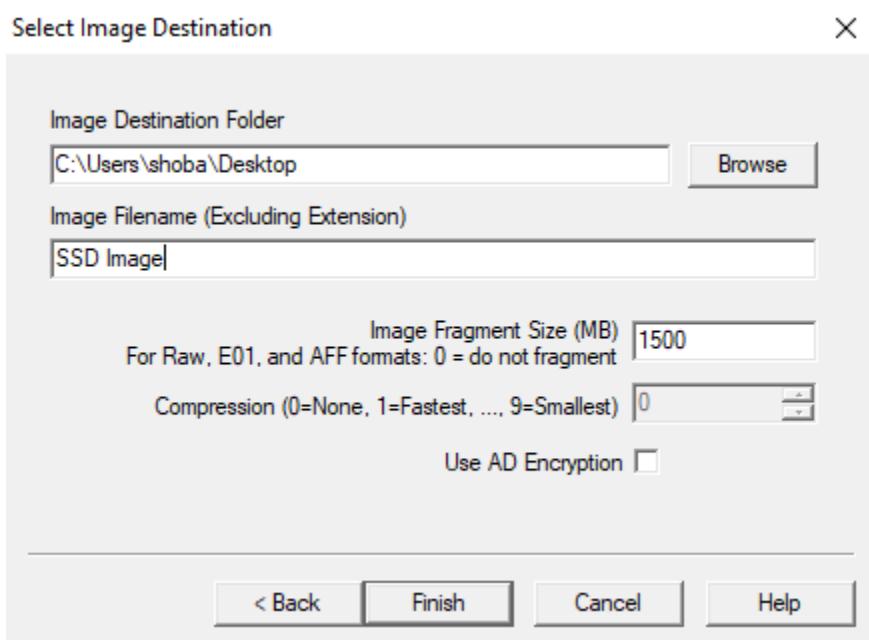


Figure 59. Selecting the Image Destination

Clicking on finish would create an image:

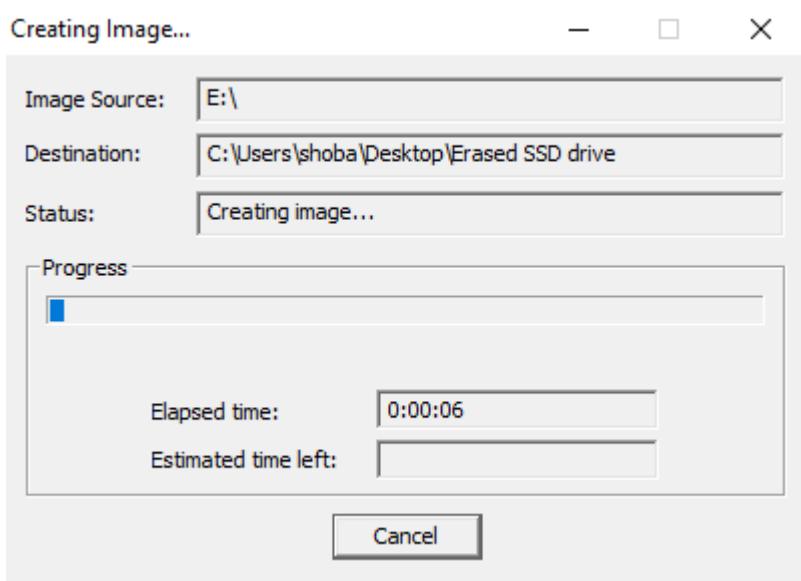


Figure 60. Creation of Image in Progress

Summary

In this chapter, we have loaded the data into the drives and created images using FTK Imager. Later, we have loaded the images onto the Forensic toolkit and analyzed the results with data on the disks. Then, the data is completely erased from both the drives, created images for the empty drives and analyzed the results. In the next chapter, we compare the results and give conclusions on the obtained results.

Chapter V: Results, Conclusion, and Recommendations

Introduction

In this chapter, we will be comparing the results obtained and derive a conclusion on the findings.

Results

For this project I used a Seagate external hard drive and Western Digital solid-state drive. Then, for the next step of our process of creating an image, we used FTK imager. After the image creation, we used FTK for analyzing the data.

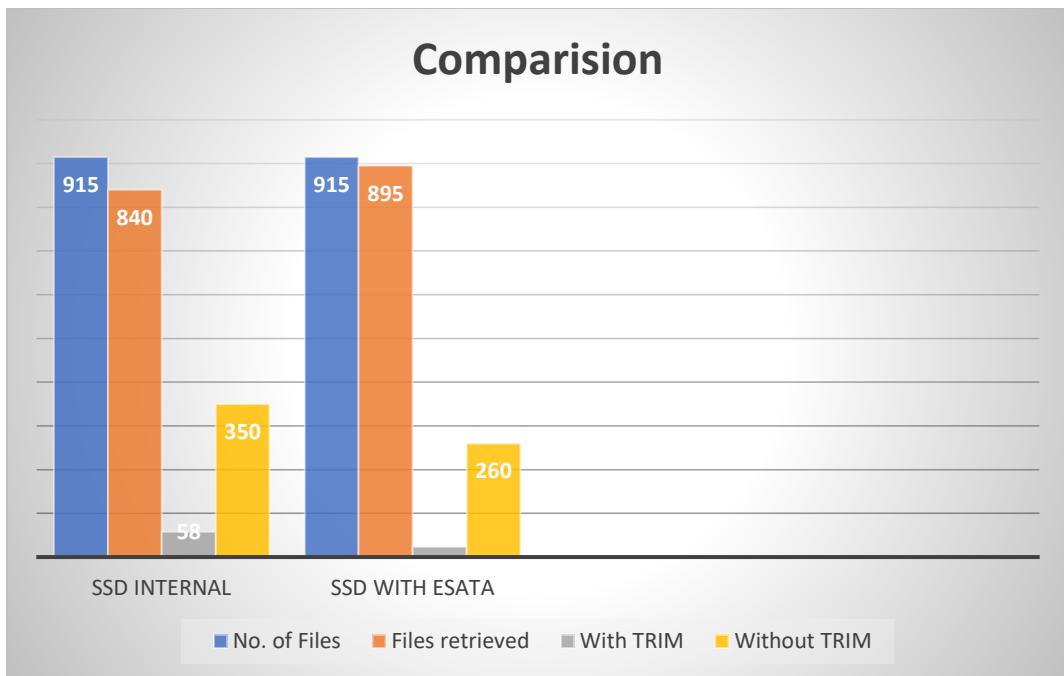
For the first step in our process we choose the Seagate External Hard drive. Then, with the help of Forensic toolkit imager, we created an image of the hard drive. Enable the Trim command by logging in as administrator from the command prompt. After this step was completed, we opened the Forensic toolkit to analyze the data. We could almost see all the files from the image file.

In the next step we disabled the trim command and created the disk image with the help of FTK imager. Analyze the image file using the FTK and see the results. We saw that there was not a lot of change in the files. Thus, we concluded that Trim function was not effective in HDD.

Coming to the next stage in our experiment, we choose the Western Digital Solid-State drive. Then, with the help of Forensic toolkit imager, we created an image of the solid-state drive. Enable the Trim command by logging in as administrator from the command prompt. After this step was completed, we opened the Forensic toolkit to analyze the data. From our analysis we saw that 32 files were displayed.

Device Used	No. of Files	TRIM Enabled	TRIM Disabled
SSD	915	90% less variance with original files	40-50% variance with original files
SSD with ESATA	915	93% less variance with original files	50-60% variance with original files

In the next step we disabled the trim command and created the disk image with the help of FTK imager. Later, analyzed the image file using the FTK and saw the results. We saw that there is almost 90% variance in the file count. Thus, we can conclude that Trim function is effective in SSD and is a potential risk for forensic investigation.



Conclusion

From our experiment we concluded that the emerging technology of various drives, there are challenges for forensic analysis. Existing forensic tools can retrieve data efficiently from the hard disk drives but is less effective when SSD's come into play.

During our analysis we observed that Trim function had erased 90% of the files from the allocated storage space in SSD. The comparison of file retention across Trim enabled drives showed that the files are unrecoverable. The experiment has also been done using the external SSD with ESATA wire connected to the computer which has resulted in more unrecoverable files. But, in contrast for hard disk drives, as Trim function is not available, there was 0% effect on the files.

Future Work

As there is an increase in the use of SSD's, the forensic investigators are facing several issues in retrieving the lost data. So, there is a higher scope that various new forensic software's and tools come into play for retrieving the lost data.

As a part of this I would extend my research in how effective the trim function would be in the future and how much percentage of the files can be retrieved if the trim function is enabled or disabled.

References

- Abdullah Al Mamun, G. G. (2007). *Hard disk drive mechatronics and control*. Florida: Taylor and Francis Group.
- Blackburn, J. (2012). *Anatomy of a solid-state drive*. New York: ACM Digital Library.
- Boddington, B. B. (2010). Solid state drives: The beginning of the end for current practice in digital forensic recoverygraeme. *The Journal of Digital Forensic Security and Law*, 5(3), 1-21.
- Cactus Technologies. (2017). *Solid state drive*. Texas: Protofuse.
- Choi, K. (2010). *NAND flash memory*. Santiago, Chile, Samsung Electronics, Co. Ltd.
- Christopher King, T. V. (2011). Empirical analysis of solid state disk data retention when used with contemporary operating systems. *The International Journal of Digital Forensics and Incident Response*, 1-7.
- Data Recovery. (2014). *How does a hard disk work*? Retrieved from Data Recovery tips:
<http://data-recovery-tips.co.uk/hard-disk-work/>
- DFRWS. (2001). *A road map for digital forensics research*. Retrieved from Digital Forensic Research Workshop : <http://www.dfrws.org/>
- Digital Forensics. (n.d.). In *Wikipedia*. Retrieved from
https://en.wikipedia.org/wiki/Digital_forensics
- Draalin. (2013). *What makes the SSD innovative*. Retrieved from <https://draalin.com/makes-ssd-innovative/>
- Fujitsu Technology Solutions. (2014). *Solid state drives*. Fujitsu PRIMERGY Servers.

Fulton, J. W. (2014). *Solid state disk forensics: Is there a path forward?* Ann Arbor, MI: ProQuest LLC.

Geier, F. (2015). *The differences between SSD and HDD technology regarding forensic investigations.* Sweden: Linnaeus University.

Hard Disk Drive (HDD). (n.d.). In *Wikipedia*. Retrieved from Wikipedia:

https://en.wikipedia.org/wiki/Hard_disk_drive

Hubbard, B. R. (2016). Forensics analysis of solid state drive(SSD). In *Proceedings of 2016 Universal Technology Management Conference (UTMC)* (pp. 1-11). Minnesota.

Hutchinson, L. (2012). *My SSD does garbage collection, so I do no need TRIM... right?* Ars Technica. Retrieved from

<https://arstechnica.com/civis/viewtopic.php?t=1281497&start=80>

IBM. (2015). *IBM 350 disk storage unit.* Retrieved from IBM: https://www-03.ibm.com/ibm/history/exhibits/storage/storage_350.html

Intel.com. (2017). *Intel high performance solid state drive - Advantages of TRIM.* Retrieved from Intel: [https://en.wikipedia.org/wiki/Trim_\(computing\)](https://en.wikipedia.org/wiki/Trim_(computing))

Kopchak, T. (2016). Do SSDs have mind of their own? *DEFCON 24* (pp. 5-10). Las Vegas: DEFCON Conference.

Michael Cornwell, P. S. (2012). *Anatomy of a solid-state drive.* Retrieved from acmqueue:
<http://queue.acm.org/detail.cfm?id=2385276>

Micron. (2008). *Wear-leveling techniques in NAND flash devices.* Austin, TX: Micron Technology.

Ngo, D. (2013). *Digital storage basics*. Cnet. Retrieved from <https://www.cnet.com/how-to/digital-storage-basics-part-1-internal-storage-vs-memory/>

Nitin Agrawal, V. P. (2002). *Design tradeoffs for SSD performance*. California: Usenix.

Rent, T. M. (2010). *SSD Controller*. Retrieved from

https://www.storagereview.com/ssd_controller

Solid state drives (SSD). (n.d.). In *Wikipedia*. Retrieved from Wikipedia:

https://en.wikipedia.org/wiki/Solid-state_drive

Wear levelling. (n.d.). In *Wikipedia*. Retrieved from Wikipedia:

https://en.wikipedia.org/wiki/Wear_leveling

Yuri Gubanov, O. A. (2014). *Recovering evidence from SSD Drives: Understanding TRIM, garbage collection and exclusions*. Palo Alto, CA: Belkasoft.