4-2020

Forensic Research on Solid State Drives using Trim Analysis

Rusvika Reddy Nimmala
nrusvikareddy@stcloudstate.edu

Forensic Research on Solid State Drives using Trim Analysis

By

Rusvika Reddy Nimmala

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

May, 2020

Starred Paper Committee:
Mark Schmidt, Chairperson
Lynn Collen
Sneh Kalia

Abstract

There has been a tremendous change in the way we store data for the past decade. Hard Disk Drives, which were one of the major sources of storing data, are being replaced with Solid State Drives considering the higher efficiency and portability. Digital forensics has been very successful in recovering data from Hard Disk Drives in the past couple of years and has been very well established with Hard Disk Drives. The evolution of Solid State Drives over Hard Drive Drives is posing a lot of challenges to digital forensics as there are many crucial factors to be considering the architecture and the way data is stored in Solid State Drives. This paper gives a very detailed picture of the evolution of Solid State Drives over Hard Disk Drives. We understand the differences in their architecture and the ways to extract data from them. We further discuss in detail the various challenges Solid State Drives pose to the field of digital forensics, and we try to answer contradictory beliefs those are 1) Would data be permanently deleted in a Solid State Drives destroying the forensic evidence required to solve a case? 2) Can data be restored in a Solid State Drives by using proper techniques and still can be used as evidence in digital forensics? In this paper, we talk about the introduction of concepts such as the TRIM Command and Garbage collection, their importance, and we set up an experimental scenario where we implement the TRIM command and try extracting data from different types of Solid State Drives. We compare and evaluate the results obtained through the experiment and try to analyze the uses of the TRIM command and its performance over various Solid State Drives. The paper also discusses future work to make the role of Solid State Drives more efficient in digital forensics.

Table of Contents

Chapter Page

Chapter Page

Chapter Page

List of Tables

List of Figures

Chapter I: Introduction

What is Forensics?

"*Forensic science, when stated by Wikipedia, is the application of science to criminal and civil laws, mainly on the criminal side, i.e., during an investigation*" (Forensic science, n.d). Forensic scientists generally collect, preserve, and analyze the data which they get at the forensic site at the time of the investigation.

Digital forensics

Year after year, the usage of computers and other digital devices has been increasing. Today, computers act very important in people's lives; they are like the right hands. Computers are used almost in all fields. Every person's life would be horrible and challenging to imagine if they don't have computers. Understandably, the computer has tremendous advantages.

But on the other hand, computers and all other devices are used for unlawful actions that provide a path for fraud and give chances for committing crimes. Illegal activities that are done with the help of computers are hacking, fraud, internal computer crime such as worms, and theft with the help of hardware or software. There are two different ways of committing a crime with the help of a computer. The first one includes committing a crime with the help of a computer system. In this category, the crimes did not occur until the birth of computers, and for committing such crimes, computers are essential. The other type of computer crimes are vast in numbers and include crimes that have been existing for centuries, but for now, they are committed using a computer system.

Digital Forensics came into the picture when there was a rise in computer-related crimes. It was a new branch of forensic science, and it deals with the modification of digital evidence from digital devices in a way that is judicially acceptable by the court. "*Digital forensics can be defined as a collection, preserving, analysis, and court presentation of computer-related evidence*" (Patzakis, n.d). Forensics generally involves the creation of bitstream copies of digital storage to secure the integrity of data and to encapsulate the data, which could have been lost in a logical copy.

Digital Evidence

The emergence and penetration of computers and all other devices have created a massive impact on laws and jurisdiction in people's everyday lives for the past few years. Traditional evidence is not the only evidence that is being used nowadays. Digital evidence such as videos, files, photos, etc. is the primary evidence to be provided against a criminal. Digital evidence has many sources such as network servers which include emails, social networks, and websites (these are the supporting applications); computing devices such as laptops, desktops, music players, digital cameras, cellular telephones; network hardware like routers (this the backbone of the internet) which are available at homes, companies.

A lot of trails and traces are left behind when an attempt is made to acquire electronic information against the rules of privacy and confidentiality defined by law. Criminals can be convicted in the court of law on producing proper evidence, which can be obtained by a set of proven practices.

The term digital evidence means "*any probative information stored or transmitted in digital form that a party to a court case may use at trial"* (Casey, 2004). Digital evidence includes

all the digital data through which we can prove that a crime has been committed or provide information confirming the relation of the crime to the victim or the perpetrator.

Figure 1. Different types of digital evidence *(Slideshare, n.d)*

Integrity and Dependence of Digital Evidence

The court procedure includes providing all the evidence which meets the specified legal requirements. To provide the evidence in court, they should follow the five properties. The foremost characteristic is that digital evidence should be *admissible.* It means that the evidence which has been collected should be in proper condition so that it can be used in court. If we fail to fulfill this requirement, then it is equal to not collecting the evidence. Due to which the cost is higher. The next one is *authenticity*. To show the evidence, it must be connected to the incident, which means whatever we are exhibiting should be appropriate to the incident. There is another property known as *completeness*, which directs us to the admissibility of digital evidence. It is not at all favorable to collect evidence according to an individual's viewpoint. Evidence should be collected in such a way that they have attackers' actions and also have evidence to prove his innocence. The last but second characteristic is reliability. The important thing to keep in mind is

that the evidence's authenticity and veracity should not be doubted based on the collection of evidence and analysis of procedures. The last property is *believability*. Whatever evidence that is being produced in the court should be unambiguous so that it can be understood and believed by the jury members. If the jury does not have any idea of what they are showing, then there is no point in presenting the evidence.

The process of Digital Forensics

The digital forensic process includes (Security, 2009):

1.Collection 2. Examination 3. Analysis, and 4. Reporting

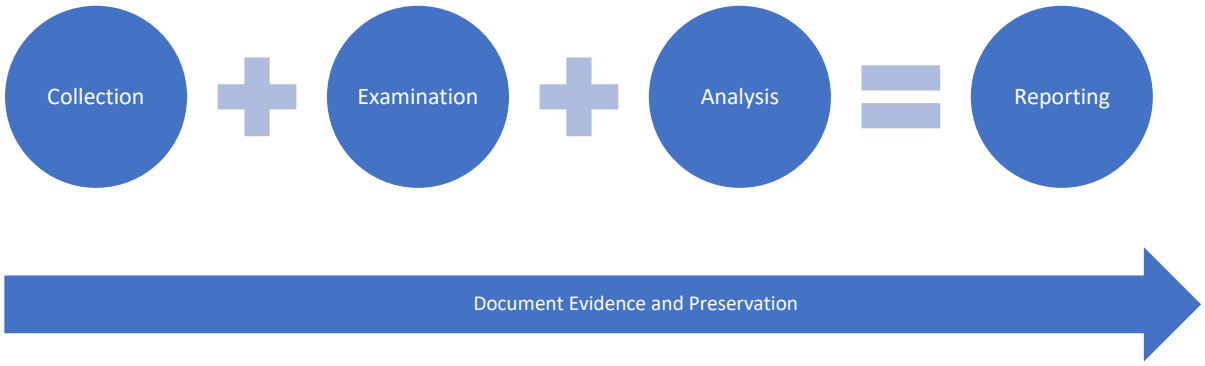

Figure 2. Forensic Process *(A Comprehensive case study on digital forensic, n.d)*

- **Collection**: Identity, isolate, label, record, and collect the data and physical evidence that are related to the incident being investigated while establishing and maintaining the integrity of evidence through chain-of-custody.
- **Examination**: Identify and extract relevant information from collected data, using the appropriate forensic tools and techniques, while continuing to maintain the integrity of evidence.

- **Analysis**: Analyze the results of the examination to generate useful answers to questions presented in the previous phase. The case is typically being solved in this phase.
- **Reporting**: Reporting the results of the analysis is made, which includes findings that are relevant to the case, actions that were performed, actions that are left to be performed, recommended improvements to procedures, and tools. (Security, 2009)

Pros and cons of Digital forensics

Information is being spread all over the internet every single day. This seems like an advantage to us, but it allows criminals, hackers, etc. "*Phishing, corporate fraud, intellectual property disputes, theft, breach of contract, and asset recovery are some of the situations where computer forensics is being used*" (Pros And Cons Computer Forensics, n.d). Technical and legal issues are involved in this process. The evidence which is being presented in court is investigated in such a way that it is admissible in court. The illegal matters which are involved with the digital forensics are dealt with only when they have physical evidence. In digital forensics, they usually have electronic evidence, which was an advantage because it helped in retrieving the lost, deleted, or damaged data of the case. The main advantage of digital forensics is that it can search and analyze tons and tons of data by searching for keywords in the hard drive in any language possible quickly and efficiently. This is an added help to the investigators because cybercrime is all over the world. Retrieving the relevant data that criminals have lost and deleted, became an important proof in the court. Legal professionals were able to produce data in the court, which was previously impossible.

When we make use of digital evidence or any electronic evidence to show in the court, it becomes one of the disadvantages because whatever evidence we show should be justifiable. The data which is to be presented can be easily changed, so the investigators are required to fully bind with the standards of the evidence presented in the court. The data which is shown should be mitigated. The forensic analysts must be trained about the legal standard procedures which are to be followed when they are to handle evidence. Another drawback is the money spent while retrieving the data. Forensic experts are hired on an hourly basis. So basically, the analysis and making of the report can take up to 15-20 hrs., but it can also take fewer hrs than expected because it depends on the case. The other disadvantage is that the investigators negligently might have disclosed some of the authorized relevant documents while retrieving data. The person who is involved in the case must know about digital forensics. Not knowing may cause problems for them because they must cross-examine the expert's witnesses. The same rules apply to judges, solicitors, and barristers. The analyst’s job is to covey his/her findings in a better and understandable way to everyone.

Problem Statement

As technology is evolving at a very fast pace, it also poses many challenges to the field of digital forensics. Because it may take much time to update the laws as there are many factors and parties involved, it is also crucial that we identify the immediate changes happening in the technical world and to identify the alternative measure which helps us recover digital evidence in a way that it has not been tampered with and also making sure that the evidence serves its purpose in identifying the right victim and perpetrator related to the case. In this paper, we will be looking into the advancement of Hard disk drives into solid-state drives. We will also discuss their

architectural differences and compare them to each other in terms of reliability, efficiency, accuracy, etc. The primary purpose of the paper is to understand the challenges posed by solid-state drives and to understand the approaches such as the TRIM functionality, garbage collection, wear leveling, encryption, which help retrieve as much as relatable data possible.

Nature and Significance of the Problem

The work of HDD data retrieval for the researcher is much simpler and less complicated in comparison to SSD data retrieval, as some SSDs are created with NAND flash memory. According to the figures, the use of SSD is substantially higher. Thus, the comparison of HDD versus SSD forensic analysis allows researchers and investigators to take more appropriate steps when conducting an SSD forensic analysis.

Objective of the Study

The aim of the paper is to find out why it is difficult to retrieve data in SSDs when compared to HDDs. The study will compare results when TRIM is enabled and disabled and how each of them makes the situation worse for a forensic investigator at the time of the investigation. This research also finds out if data is permanently deleted in an SSD destroying the forensic evidence required to solve a case and can information be restored in an SSD by using proper techniques and still can be used as evidence in digital forensics.

Study Questions

1) Do SSDs create forensic difficulties?
2) Are new files being overwritten on the old blocks (with the erased file data)?
3) Is TRIM enabled or disabled helpful for retrieving deleted files?

4) What problems are faced during data acquisition with TRIM functionality?

Limitations of the Study

The reason for the analysis is to explore the challenges and processes of forensic investigations presented by using TRIM in this research. This research does not seek to alter any of the current evidence extraction or retrieval methods but instead explains whether such practices are sufficient or are not sufficient to retrieve data. The results of this research could only be accurate for these data.

Definition of Terms

Solid State Drive (SSD): A Solid-State Drive (SSD) is a solid-state architecture based electronic storage system. NAND and NOR flash memory are equipped in SSDs to store non-volatile data and DRAM. A similar purpose is shared by an SSD and magnetic hard drive (HDD). An SSD is also referred to as an electronic disk drive (Techopedia, 2017).

TRIM: A trim command enables an OS to notify a Solid-State Drive (SSD) that the data blocks are no longer used but are wiped internally. In ATA command, it is known as TRIM, whereas, in SCSI, it is known as UNMAP (Trim (computing), n.d).

Summary

In this chapter, we discuss the basics, such as what forensics is, we give a brief introduction to digital forensics, and what is the process of digital forensics. We also discuss how digital evidence is gathered and how much we should be relying on digital evidence. Lastly, we conclude by talking about the pros and cons of digital forensics.

Chapter II: Background and Literature Review

Introduction

To understand the problems involved in cracking evidence from solid-state drive compared to the hard disk drive, we need to have a better view of their functioning. In general, we know that both the solid-state drives and hard disk drives are used for storing information. In this chapter we will discuss in what way data it is stored in these drives, how data is deleted in these drives and how data recovery happens in these drives, these are the key factors for us to understand what challenges are faced by forensic investigators while retrieving information.

Background Related to the Problem

Although solid-state drives and hard disk drives are identical and have the same goal of storing information, the working of these drives is entirely different. When comparing solid-state drives to hard disk drives, the solid-state drive has a different mechanism, and it also has some extra added features. So, the forensic analysts are not able to follow the same age-old method of retrieving evidence which was very successful in the past.

Literature Review Related to the Problem

Hard Disk Drive (HDD)

Hard drives came into existence at around the 1950s, and still today, they are the primary form of data storage in the present-day world. Most of the people have hard drives in their personal computers for accumulating the dominant part of their data even though the usage of flash memory has been increasing. We are lucky enough if we get a hard drive for our investigation because there can be a colossal amount of relevant data living within it. But chunking the information together

and getting answers for questions like what the hard drive was used for, when the data on it was created, and by whom it was done can be very difficult-specifically if the data had been reformatted if data has been deleted from the hard drive or the user has attempted to physical damage or destroy the drive (Digital Forensics for Hard drives, n.d).

Architecture and operation of HDD

HDDs are the primary storage solutions for all the system and application software and also for the private data (e.g., files, folders, pictures, etc.) in everyday computing environments. HDD has a rotating magnetic media, which is in the shape of a disk and is called a *platter*.

The Platter is shown below. The platter's functionality is to rotate basically. In one second, it goes for several hundred rotations. It also contains a magnetic domain where data is written. In-depth observation inside a platter exposes us to a sliced division. Each slice is known as a *sector*; this shows us the least possible addressable area of the HDD, which is around 512 B. Sadly, the frequent drawbacks of HDD are due to these small moving parts.

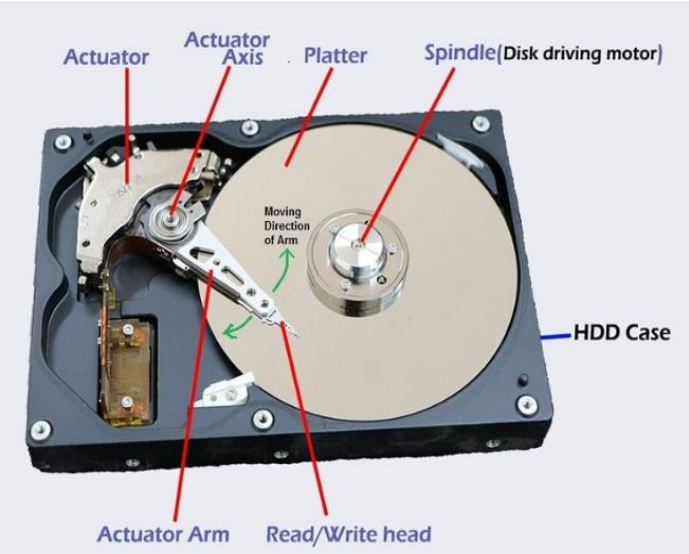

Figure 3. Parts of HDD *(HDD Parts, n.d)*

A brief understanding of the storage devices which we use to store data can guide us in what way we can preserve data. A hard substance that is covered with a coating of a magnetic component is a platter (Yohannes, 2011). There are coordinated circles on the surface of the disk; these are magnetic, and data is stored on them, they are called tracks. The drive consists of various platters that are bundled upon one another, and the correct amount of space is left between the platters for reading/write heads. Typically, both sides of the platters are stocked with data. The platters are connected with a spindle that is attached to a motor.

The platters are moved to a particular place when the head actuator assembly is moved due to read /write heads. All heads move in a bunch and read/write heads are there on each side of the platter. The actuator looks for the position on the platters called *cylinders.* At a particular location, all the tracks are bundled upon one another, which is contained in a cylinder. At one point, only one platter head can do the read or write functions.

A Block is the intersection of a track and a sector, which is the minimum addressable size of an HDD. This is done by specifying three things: The Cylinder, The Head number, and The Sector number.

Data arrangement on hard disks

The data which is documented on a magnetic media is as small as one bit. The arrangement of these bits is in the form of circles that are placed on the tracks around the disks. The exterior side of the disk consists of around 70,000 to 100,000 tracks on an ordinary hard drive.

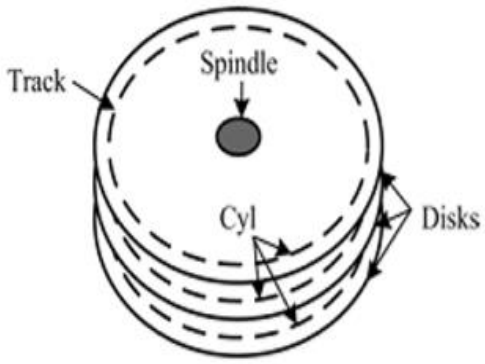

Figure 4. Tracks and Cylinders *(Geier, 2015)*

To write on a new track, the write head is moved by the arm to the next position on the radius. All data is written in data blocks of 512 bytes which are recorded sequentially along the track (Geier, 2015) The architecture of a hard disk consists of many disks which are recordable on both sides and is made possible with an actuator arm with multiple sliders and heads. All the surfaces are named from 0, which is the outermost track. All the tracks are allocated into cylinders, and each cylinder consists of tracks with the same numbers. The access speed can be increased by manufacturing multiple heads simultaneously. All the tracks have servo sectors, which are the divisions of tracks and are of 512 bytes, each starting from 1 for each track. The sectors and tracks are identified using various magnetic patterns which are integrated during the build by the manufacturer during the time of production.

Cylinder-Head-Sector (CHS), is the addressing method used to address sectors. CHS helps to identify a sector using the cylinder starting from 0, which is the head of the according head and the sector, which starts from 1. LBA, Logical Block Addressing have replaced this method of addressing.

The disk must be formatted, and partitions must be appropriately created before storing any data on the disk. The logical unit that divides the disk into various logical parts is known as a partition. The partition table is stored on the first sector of the disk in a Master Boot Record (MBR), which tells the operating system how the disk is divided. The file systems over partitions vary widely based on the operating systems. Operating systems like windows use FAT and NTFS while Linux uses EXT and EXT2. The location of the data stored on the physical disk is located with the help of the file system. Windows use a master File Table (MFT) as an index of all the files stored on a hard disk. It is not true that the data is deleted on reformatting or deleting the partition. It simply deletes the file allocation table (FAT), but the data is still available for recovery using a proper process. Figure 5 shows the disk structure containing two partitions.

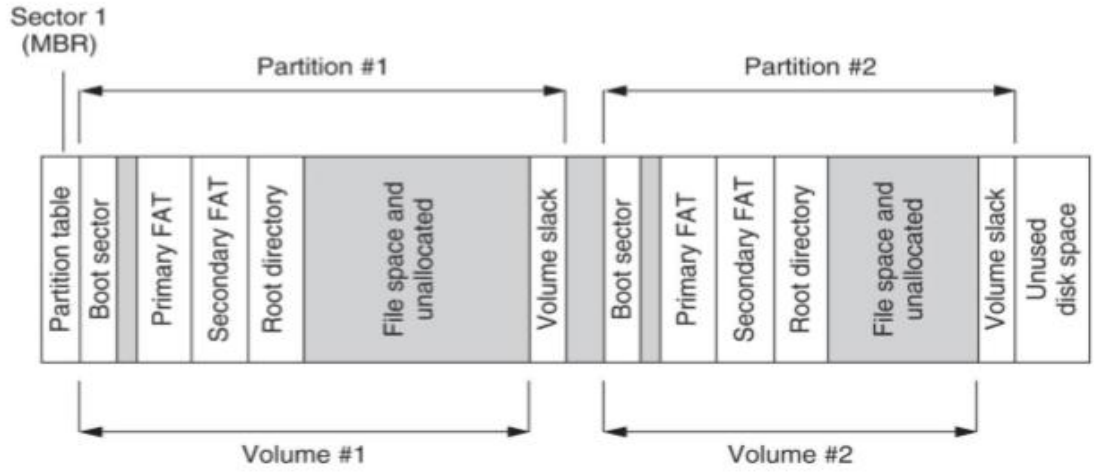

Figure 5. Depiction of disk structure *(Geier, 2015)*

How is Data deleted in HDD?

The following are the methods to delete data from HDD:

Boot and nuke method. A computer technician depicts that the software, i.e., Darik's Boot and Nuke is an open-source boot disk utility. It generally helps a lot of disk wiping methods and performs from inside the computers RAM, helping it to brush the disk thoroughly.

1. Firstly, we have to download Darik's Boot and Nuke (DBAN). There are two different versions one for PCs and the other one for Macs.

2. We know that DBAN is an ISO file, so we need to use burning software that burns the ISO files. After Burning the file on to the CD, we have to check if we can see the "ISOLINUX" folder on the burned CD. If it doesn't consist of the required folder, then our hard disk cannot be erased.

3. Now we must put the CD on the computer for which we are erasing the hard drive while we restart it. It should boot directly from the CD, but in the worst cases, if it doesn't, then we need to adjust the boot order in the BIOS. In MAC computers, we need to press the 'C' key while the computer starts up.

4. The last step includes selecting the disk from which we must delete the data. The important thing to keep in mind is to choose the right one while deleting because after deleting, we cannot recover the data. Any number of times, we can overwrite and delete it. When we overwrite with "one pass random data," it prevents the recovery of data.

Physical Destruction Method. A physical Destruction is a good option for an archaic drive for which you don't have the necessary interface on a computer to connect it to, or if the drive will not reliably boot for you to run a software-based erase (How to Permanently Erase Data Off a Hard Drive, 2019). An added advantage is that this data cannot be recoverable by forensic investigators as well.

The steps involved in this process are

- Firstly, remove the old hard drive that we want to dismantle from a computer or external enclosure, such as the case around the USB hard drive.
- We need to unscrew all the screws then holding the top. In rare cases, there might be an air seal. We need to remove that.
- After we remove the top, we see a few silver disks, which are called as platters. Now start putting scratches on the platters with Torx wrench and start smashing it with a hammer. Doing on a hard surface is recommended. The safety tip, while doing this process, is to wear glasses to protect against flying glass platters.

Figure 6. Destroyed Hard disk and a hammer *(Physical damage, n.d)*

Selective File Wipe Methods. This method is not as good as Boot and Nuke or physical destruction, but it can be used to erase the unused space when the computer is not functioning. This method is differently used on windows, MAC, and Ubuntu operating systems.

- Windows

  Microsoft Sdelete: It keeps a check on deleted files, directories and cleans up the free space.

  Wipe File: This file overwrites the file which we would like to erase.

  DeleteOnClick: It has a “Secure Delete” option, which overwrites the files.

  Eraser: It is expected to perform overwrites in regular intervals on empty disc space to get a hold of the orphan files.

  WBD (Wipe Bad Disk): It wipes disks with bad sectors.

- MAC OS

  Permanent Eraser: It is a substitute for the “Secure empty trash” option. Thirty-five times a file can be overwritten.

  Disk Utility: A function called “Erase free space...” is there in this which writes on the unused space 1,7, or 35 times.

  srm: It is a command prompt command which can delete and overwrite the files. This makes a recovery absurd.

- Linux/Ubuntu

  Wipe package from Ubuntu Unleashed: It can add secure on multi-pass file delete, just like DeleteOnClick in windows.

How does data recovery happen in HDD?

The hard drive has the capability of storing and transferring data a lot simpler. Data loss on a hard drive might happen due to clicking on format option, hardware failure, or due to any virus attack. We can recover data from dead or damaged or from a formatted hard drive.

The following are how we can recover data from a hard drive:

- ✓ Using Command prompt

  The command prompt is a basic command which is utilized to recover files through an external hard drive.

  1. First, we have to connect the external hard drive into the USB port on the Windows operating system.
  2. Next, we have to press the “Windows” and “R” button on the keyboard at the same time to activate the run box.
  3. When the run box opens up type “cmd” and clicks ok.
  4. The next step in command prompt is to type " attrib -h -r -s /s /d [drive letter]:*.* "and click enter(drive letter means whichever drive you to want to select while recovering).

- ✓ Recovering data from external hard drive with external hard drive recovery tools

  FonePaw Data Recovery tool can recover files from external and local hard drives, partition hard drive recovery, memory card recovery, supporting hard drive recovery, and so on (Green, 2018).

  The important thing to keep in mind is

1) We should not perform any operation such as delete, move, or add data to the external hard drive till we recover the data, which we need because any activity on the hard drive will overwrite the old data on the drive.
2) If we want to use any recovery tools, do not download the program on the hard disk. We have to download it on the computer.

The steps involved are as follows:

- Recovering file types to be selected

  After we install the recovery tool on to the computer, we have to launch it. After plugging in our external drive to the computer, the hard disk will be detected in the "removable drive." In this step, we have to select all the files which we want, like images, audio, video, email, documents, and so on. Then we have to click on scan.

- Previewing lost files

  After the scanning is done, the data on the external hard drive will appear on the typed list. The essential files which we want can be check boxed with a tick mark. The necessary thing to keep in mind is that if the target files didn't show up, then we can do a "Deep Scan" mode to get deep scanning done on the hard disk, and this process takes a lot of time like literally many hours.

- Selected files to be recovered

  When we complete the selection of all the target files, we can click on the "Recover" button. After some time, the data which is on the external hard disk will be recovered on to the computer.

Figure 7. Data recovery *(Zhang, 2018)*

Challenges of HDD

- It consumes a lot of power.
- Resistiveness for shocks is pretty low.
- The size is enormous, and while recovering data, it is very hard.
- Controller cards (SCSI) might be needed.
- Very loud automated noises are generated.
- If the jumper settings on a hard drive are not proper, the hard drive might be burned.

Solid State Drive (SSD)

Figure 8. SSD *(Varinder, 2016)*

Solid State Drives is an upcoming technology to store data endlessly and is gradually replacing the traditional hard disk drives. SSDs differ a little from HDDs. A Solid-state drive is used for storing data that uses flash NAND memory. This is the most basic element for storing data on SSD for an elongated duration. As SSDs do not have electromechanical elements, just like HDDs, they are faster than traditional HDDs.

The data in SSDs is stored in microchips, which is similar to data storing in USB flash drives. Storing of data and recovering files is done immediately, and it does not need to wait for moving parts to position on the required sector of the magnetic platter (Zubair Shah, 2015). In IT culture, this is the most common storage device used, and it is anticipated to take over HDD soon shortly.

Architecture and operation of SSD

Flash memory based SSDs are usually built on an array of flash memory packages to avoid the limited bandwidth provided by individual flash memory package. We can achieve a higher bandwidth accessing in a parallel fashion as the flash memory chips can be striped over, which is similar to RAID-0 storage. The controller is connected to the flash memory package using an I/O serial bus. Connection interfaces such as SATA are used to send the requests from the host, which are later received and processed by the controller, which also assigns instructions to transfer the data to the flash memory array from the I/O devices. To read a page, the data which was initially obtained from the flash memory array is transferred from or into the register of the plane, and then the controller receives it through a serial bus.

To reverse the direction of the data flow, we use a write command. Some SSDs can also buffer to cache data or metadata as they are equipped with an external RAM.

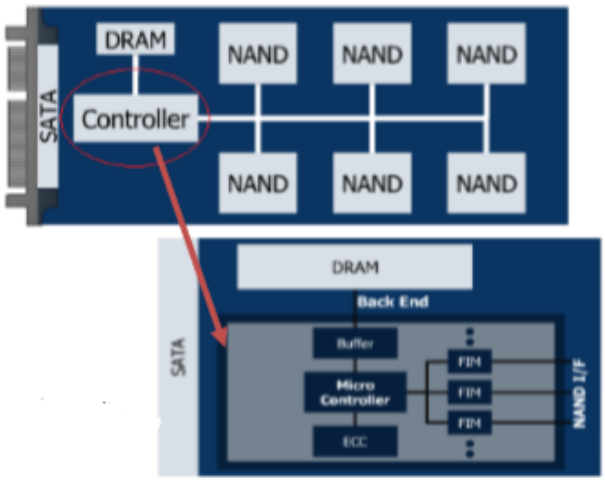

Figure 9. SSD architecture *(Yohannes, 2011)*

The NAND flash memory package is composed of one or more dies (chips). Each die is segmented into multiple planes. A typical plane contains thousands (e.g., 2048) of blocks and one or two registers of the page size as an I/O buffer. A block usually includes 64 to 128 pages. Each page has a 2KB or 4KB data part and a metadata area (e.g., 128 bytes) for storing Error Correcting Code (ECC) and other information. Exact specification data vary across different flash memory packages (Yohannes, 2011).

"*Arrays of cells are grouped into a page, arrays of pages are grouped into blocks*" (Yohannes, 2011).

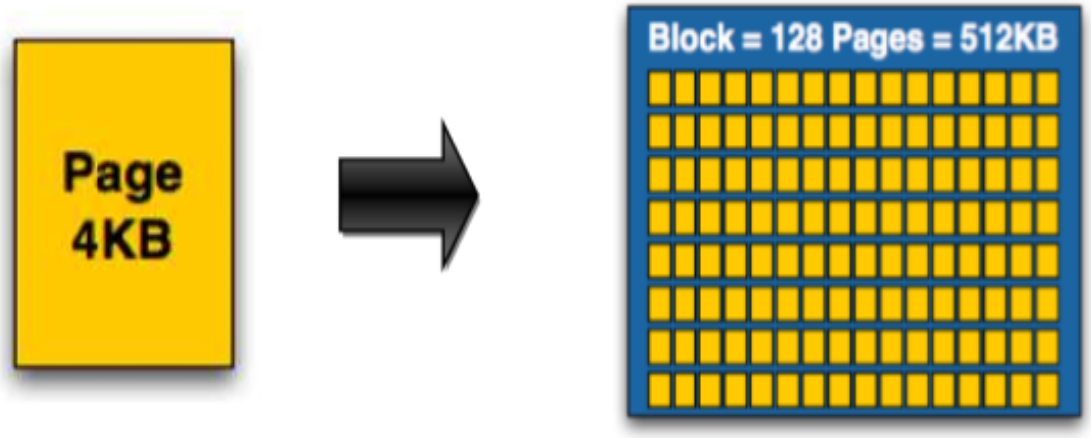

Figure 10. Representation of pages and blocks *(Yohannes, 2011)*

Blocks are then grouped into planes, and you will find multiple planes on a single NAND flash die.

The three significant operations, read, write, and erase, are supported by the flash memory. Each read operation is performed in the units of pages and could take 25μs (SLC) up to 60μs (MLC). All memory cells on the similar word line consist in the smallest area of the flash

memory known as a page, which also supports the write operation. The smallest is that it can be erased in flash memory with a single operation is known as a block.

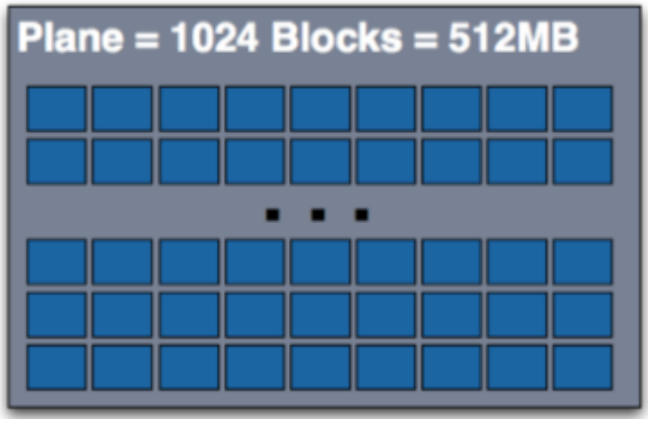

Figure 11. Organization of NAND Memory *(Yohannes, 2011)*

The Flash Translation Layer (FTL) is implemented as a part of the SSD controller through which the logical block arrays are exposed in the upper-level components and is also used to emulate the hard disk. The Flash Translation Layer (FTL) is considered to be a very critical component as it plays a very major role in optimizing performance in SSDs by adopting a lot of sophisticated mechanisms.

The most major part of SSDs is the controller, which is considered as the brain and is built up of various elements such as Flash Interface Modules (FIMs), Microcontroller, Buffer, and an Error-correcting code memory (ECC). The individual NAND Flash devices are connected both logically and physically by FIMs, each of which is capable of communicating with multiple NAND Flash components. We can extend and increase the performance by adding more FIMs to the SSDs. As SSDs are very new in the field of technology and all the manufacturers have their proprietary rights over the way they build SSDs, which makes the internal architecture a secret. It becomes an

even bigger concern considering the competition among the vendors to produce better and more efficient SSDs. This makes it difficult for us to determine the exact life of SSDs. Though we can come up with an expected list of all the structures and mechanisms to work with, we cannot establish a definite conclusion until the hidden techniques used by the manufacturers become an open-source to the public. For now, we can consider SSDs as mystery devices, but we cannot tell the number of mysteries it holds.

How does data deletion happen in SSD?

SSDs working is very different from traditional hard drives, specifically in terms of reading and writing processes on the drive. The best way to delete hard disk drives is by overwriting the space with data, which is a pointless concept to do in SSDs because of its design.

If we delete the data by overwriting (the way it is used in HDDs), it secures the data by not getting recovered by data recovery tools. This particular technique is not working on SSDs, as it is not likely to indicate a location to overwrite.

These are the following ways the data on a solid-state drive can be deleted:

File Deletion. This is one of the straight forward ways for deleting data on solid-state drives. But this method of deletion of files on the Windows operating system is not capable of protecting data from recovery software. One of the recovery tools named Recuva has found roughly 100% of the deleted files from the Windows operating system. So, this option is not the best way to delete data permanently on solid-state drives.

Solid State Drive Formatting. Out of all the available options, this is the simplest of all of them. It can be done without actually using extra software. In windows, the person should first check where SSD is in windows explorer, then right-click it and from the choices available click on format. But it is necessary to see that we don't click on a quick format because if we do click on that option, all the data on the drive will not be formatted properly. After the full format is done totally, the windows operating system will not list any files on the drive.

We could check if the files which are deleted can be restored or not after the formatting of the drive. We can check by using a recovery tool called Recuva. The process is simple here; we have first to select the solid-state drive letter and click on scan. Over here, the deep scan must be done, and the scan will take time depending on the size and speed of the SSD. We can conclude that the full format deleted all the files on the drive, leaving out unrecoverable files. It also had ignored recoverable files, but it did not have any filename, and they were all 0-byte files.

Solid State Drive encryption. Generally, encrypting the SSD should be sufficient to make all the files unrecoverable. Here we use an encryption software called True Crypt, which is used to encrypt the Solid-state drive. This software works for all operating systems like Windows, Mac, Linux.

The following is the process of encrypting a drive by using the software True Crypt.

- Firstly, we have to open the main True Crypt interface. The other option to select a drive other than system drive is a non-system partition.
- Then we have to select standard True Crypt volume and then click on the device. Now, we have to select the Solid-State Drive partition from the list of connected hard drives.

- We have to select the encrypted volume and then format it. The default values should not be disturbed in the encrypted option. Now, click on next and pick a password.
- Clicking on the format button, in the end, will give us a warning saying that all the data which is available on the drive will be deleted as soon as True Crypt volume's creation. Select "Erase any file stored on the partition." It is done by creating TrueCrypt volume inside it.
- The drive is then formatted, saying the encrypted volume has been created successfully. Recuva was made to scan on the drive; it gave an error message saying that the boot sector of SSD was not able to be read. Other recovery tools were also not able to recover files as well.

Using an HDDErase command. The erase command's function is to shift all NAND locations to the erased state; this results in removing all data from the drive. This commands job is to factory reset the settings of the drive because of which we can see decreased performance levels additionally.

This method is recommended for techy people because it involves BIOS configuration and also the creation of a boot disk. HDDErase is a tool that supports the secure erase command (Brinkmann, 2010).

The bootable disk is created. The AHCI should be disabled in computer BIOS for the HDDErase to work. Secure Erase scans the solid-state drive to check if it supports the command. After the secure erase command was used in DOS, surprisingly, no data was recovered.

How does data recovery happen in the SSD?

SSDs have complicated architecture and algorithms to track the data. SSDs are very tightly packed because they don't have any moving parts like HDDs. As they are packed closely, they are very complex. So, for recovering data quickly and understanding the issues of SSD, we use Remo recovery software.

This software has many different options, like smart scans and saves recovery sessions.

- The smart scan helps in deep scanning, which helps in looking for fragmented parts of broken files that are all over the SSD.
- Save recovery session gives you an option to save the data retrieval session on whichever location you want. The time captured to scan will be more, one reason is if the data is more and the other reason being if the solid-state drive is defective. This introduces pause and resumes functionality to recover data by saving the previous session data.

The steps to recover data are as follows for:

Category 1: accidentally deleted files and partition loss or registry errors

Firstly, we have to download the software which we are using for the recovery of data. Here we are using Remo software.

- ✓ After it is done, we have to select the "Recover partitions" option. Next, we need to pick the disk on SSD from where the data should be recovered, and later on, it should be scanned.
- ✓ We can select what type of file signature we want, and there is also an option for adding files that give us the privilege to choose what files we are looking for. We can also skip this option if we would like to recover the whole data.

- ✓ Scanning the files beforehand from SSDs partitions and extracting the selective partitions should be done from the list given. To filter our search, we can view the files through the File type view and Data type view, and we can also choose our location where we want the recovered files to pop up.
- ✓ In this, we have an option called Save recovery session, which avoids a lot of problems like avoiding rescan; if we have a damaged hard drive, we can save a lot of time with this option, and we can also resume and continue the recovery process.
- ✓ In a later stage, we can activate the software and load the earlier recovery session, which was saved to get all the lost files.

Category 2: File system failures/ corrupted MBR/ when the operating system crashes on SSD

- ✓ When we are not able to access the data due to the above reasons, it is suggested that we format the SSD.
- ✓ We use recovery software to recover the data from SSD.
- ✓ For this, we click the “Recover Drives” option.
- ✓ We need to select whether we want “Formatted or Reformatted Recovery.”
- ✓ Next, we need to select the corrupted or partitioned drive on the SSD.
- ✓ The remaining process is the same as category 1 (from step 6).

Less software is used to restore files from corrupted, formatted, RAW, or failed SSD drives using simple steps. Partition recovery can also be made if they are missing, formatted, or corrupted from SSD. If data is disappeared from partitions the reason being partitioning errors, they can be restored with the help of the software simply.

Challenges of SSDs

At the beginning of Solid-state drives, some SSDs were using similar technology as RAMs, which were installed in personal computers. Unluckily, the technology which was used faced a lot of problems that made them not to adopt like,

- The cost per individual byte was very high, which was the same as HDDs.
- They needed a stable power supply because of their volatile memory.
- They were huge, but simple to use.

SSDs major problems are:

- Before they fail to work properly, SSDs are responsible for the number of write operations to be performed. Their ability for longer life is continuously developing, and this will turn out to be a relic of the past within a couple of years, but considering few situations which require extensive writing activity may cause problems for the life expectancy of the storage devices. Due to the increased use of SSDs, people claim that these days are already behind us.
- The cost, as noted, is a lot higher for the solid-state drives than for HDDs. The price for SSDs is around $1.75 *per gigabyte*, and this only seven or fourteen cents *per gigabyte* of the storage of HHD. This way, we can conclude that SSDs are a lot expensive than HDDs.
- A vast number of security challenges for storage media that are broadly viewed as “solved issues” for HDDs are not even completely addressed for SSDs.

Security limitations of SSD

We think about flash media SSDs as the accepted implementation for our following future, but the noticeable security disadvantage about HDDs rotates around encryption and secure data deletion. So, the same applies to SSDs.

The Solid-state drives have transistors to store data. The states of transistors are divided into four of them, such as empty state or erased state and written or programmed state for data to be stored (Perrin, 2011). Every time they want to store data, they have to reset to "erased" state before they can be reset to the "written" state. For HDDs, when we want to write on an empty storage location, it requires only one operation; this way, overwriting is absurd. But for SSDs, any data which is to be written on a space must be erased first.

Hard Disk Drive Vs. Solid State Drive

SSDs and HDDs do the same activity. Their job includes booting our systems, storing our applications, and personal files. But each of them differs in one way or the other. The factors include:

- ***Price.*** Traditional hard drives are a lot cheaper than SSDs in consideration of dollars per gigabyte. The cost of 1TB internal hard disk is in the range of $40-$70, but for solid-state drives, the economical one for the same specifications is around $130. This concludes that for HDDs, it is 4-7 cents per gigabyte, but for SSDs, it is 13 to 15 cents per gigabyte. Hard Drives are still using older technologies, so they are inexpensive for the coming generations (Brant, 2019).

- ***Maximum Capacity.*** Even though consumer SSDs are as high as 4TB, they are very different and extravagant. We will mostly see 500GB – 1TB unit SSDs as basic drives in our personal computers. In 2019, 500GB was considered as a “base” hard drive limit, but while estimating the prices of the drive, the units went down to 128GB - 250GB for lower-valued SSD based frameworks. Clients in huge media companies and those who work in content creation require significantly more (i.e., 1TB – 5TB) drives, which are generally used in high-end systems. The more is the capacity of the personal computer, the more we can store all our files in it.
- ***Speed.*** This is an area where SSDs outshine HDDs. A Personal computer that has SSD on it will boot in under a minute, and it usually takes only a few seconds. A hard drive takes a lot of time, and it is slower than SSDs (Brant, 2019). A PC or Mac with SSD boots quicker, launches and runs applications quicker, and exchanges files or records quickly. Regardless of whether we are utilizing the PC for fun, school, or any office work, the additional speed which we get for our Pcs is the reasons for completing our things on time and failing to do them on time.
- ***Fragmentation.*** Hard drives work best for large files, as they are the ones that revolve while storing data. That way, the drives head can begin and end; it’s read in one uninterrupted motion. Fragmentation is caused when the hard drive begins to fill up, and large bits of the files are scattered on the disk platter here and there. Read and Write algorithms are enhanced to a point where the effect is decreased, but due to the effect on the performance, the hard drives are still divided into fragments. In SSDs, because there is

no physical read head, it has the advantage of storing data anywhere without penalty. Thus, SSDs are naturally fast.

- ***Durability.*** The SSDs do not have any moving parts, which are an advantage for keeping our data safe, until and unless we drop our laptop bag, or our system gets disturbed while operating. Most of the traditional hard disks do not move their read/write heads when the system is turned off; however, the drive platters are flying all over with a distance of few nanometers when they are inactivity. If we cannot handle our HDD with care, it is recommended to get an SSD instead.
- ***Availability.*** Hard Drives are most abundant in our older systems, but SSDs are ruling the modern world by getting used to high-end laptops like Apple MacBook Pro, which do not have a hard drive option even if we want to configure it. HDDs are offered in desktops and all the cheaper laptops, and this will continue for the next few years.
- ***Form Factors.*** Since hard drives depend on spinning platters, there is a restriction on how little they can be fabricated. It was proposed that they wanted to make a smaller 1.8-inch traditional hard drive that spins, but it was about 320GB, so apparently, smartphone companies had to settle for flash memory as their primary storage. SSDs have no such restrictions so that they can become smaller and smaller soon. SSDs are designed as small as 2.5 inches in such a way that they can be fitted correctly in the drive bay.

- ***Noise.*** The noise levels in a hard disk drive are based on the speed of the spinning platters in them. Though the operational noise is not a lot, even the quietest hard disk makes little noise. These noise levels are entirely omitted in SSDs as they do not have any mechanical parts, such as platters in motion.
- ***Power.*** The energy consumption levels are very low in an SSD as compared to a hard disk because there are no physical energy losses that are wasted by the friction of the drive platters or the noise generated by them. This makes SSDs more energy-saving than hard disks leading to lower energy bills. This helps it even easier to have a longer battery life considering smaller devices like tablets and laptops, which run on limited battery.

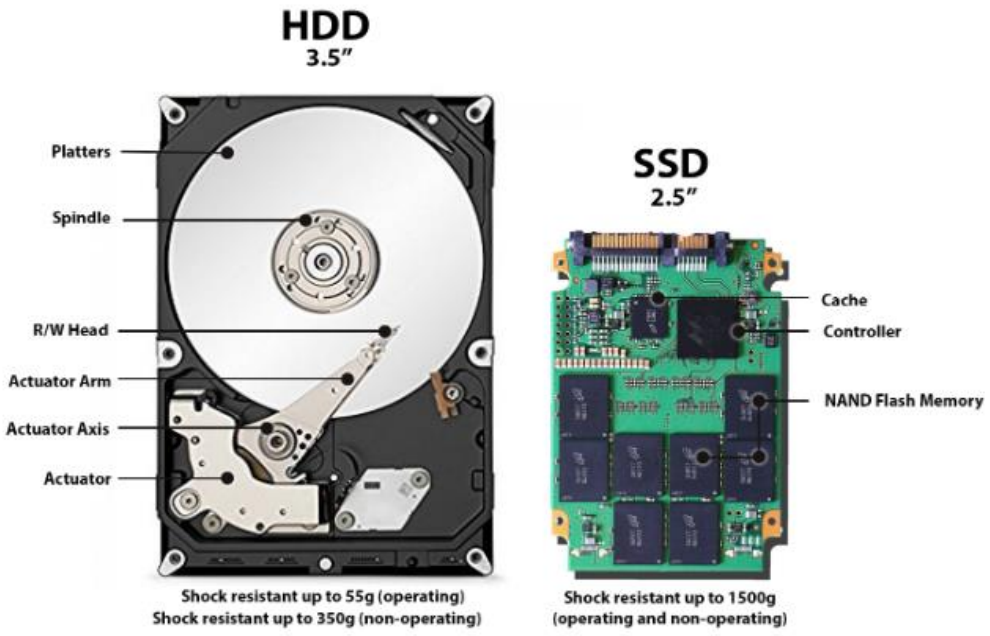

Figure 12. HHD Vs. SSD (HDD vs. SSD: What does the future for storage hold, 2018)

Table 1

Difference between SSD and HDD

Characteristic	**Solid State Drive**	**Hard Disk Drive**
Data Durability	It can be worn out based on the application they are used for.	It can wear out its mechanical parts, rendering it useless.
Startup Time	Almost instantaneous.	Disk spin-up may take several seconds.
Random Access time	As low as 0.1ms	Ranges from 2.9ms-12ms
Read latency time	Generally low but higher in cases of booting.	Much higher than SSDs
Data transfer rate	Ranges from 200MB/Sec-2500MB/sec	200MB/Sec
Read performance	Constant and independent of data location	Varies based on data location.
Cost	US$ 0.23/GB	US$ 0.04/GB
Storage capacity	Up to 512 GB	Up to 14TB
Power consumption	Equal to HDDs in DRAM models and less than HDDs in flash memory models.	Up to 20watts in a very high-performance HDD.

Literature Related to the Methodology

Features and Techniques Solid-State Drives

The features of Solid-state drives which complicate forensic analysis are:

- Wear Levelling
- Trim Functionality
- Self-corrosion
- Garbage Collection
- Encryption

Wear Levelling

Wear leveling is a technology used by some Solid-State Drive controllers to increase memory life. The theory is simple: it equally writes on all blocks of a Solid-State Drive simultaneously, so they wear out evenly. All cells receive the same number of entries, which avoids writing on all blocks.

The "wear leveling," also known as the "write amplification" concept. Since Solid State Drives write data to pages and delete it in blocks, it happens that the amount of data entered into the Solid-State Drive is more substantial than the actual update. For example, if we change a 4 KB file, we need to update and re-write the entire block that contains the file. Now we can end up typing a 4 MB data size to update a 4 KB file depending on the number of pages per block and size of our pages. The garbage collection procedure mitigates the impact of written amplification, as the TRIM command does. Maintaining a significant drive free space also reduces the impact.

Wear leveling is the technology that ensures that some NAND blocks are not written or removed in the Solid-State Drive very frequently, compared to others. While wear-leveling extends the drive's life expectancy and endurance, writing in the NAND could increase the write amplification. Blocks must often be configured and modified (to achieve the necessary number of writes) even though the user does not alter the data. The configuration and modification are done by a proper wear-leveling algorithm (Dimitrios, 2017).

Most manufacturers now use the wear leveling process to mitigate NAND flash degradation. As we noted, the distribution of data across all the SSD blocks ensures that the flash memory wears uniformly, but there is a time where the drive declines over time. A NAND single-level flash memory usually produces 50,000 programs/ erase cycles while a multi-level flash offers 5,000 cycles.

There are two types of Wear leveling:

- Dynamic Wear Leveling
- Static Wear Leveling

Dynamic Wear Leveling

Dynamic wear leveling operates on dynamically written data blocks. All new information, as mentioned earlier, is written in free data blocks, i.e., blocks not containing user data**.** Based on the number of program/erase cycles the block already has, the flash drive controller selects the new free data block. After writing the new data, the controller updates its logical internal mapping table to indicate the new physical block location. During the garbage collection process, the data block which contains the old data is marked invalid and removed and made free. The issue of Dynamic

wear leveling is addressed by repeatedly writing in the same block by moving new writing to a different physical block, thus preventing excessive Wear off of the active block (Cactus Technologies Wear Leveling-Static, Dynamic and Global, 2019).

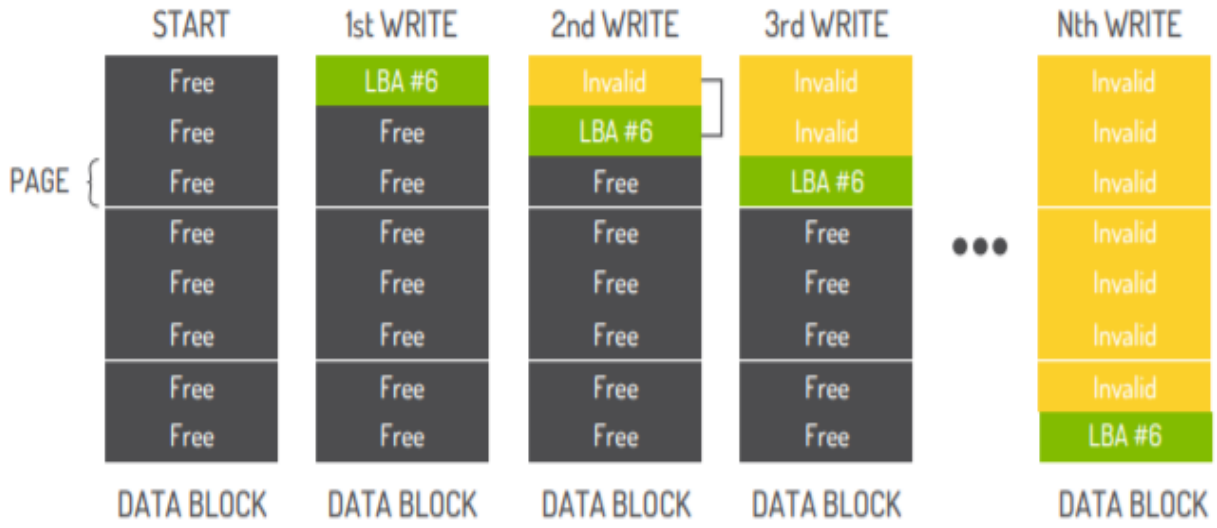

*Figure 13.*Dynamic Wear Leveling implementation (Cactus Technologies Wear Leveling-Static, Dynamic and Global, 2019)

Figure 14. Dynamic wear leveling before and after garbage collections

(Cactus Technologies Wear Leveling-Static, Dynamic and Global, 2019)

Static Wear Leveling

Static wear leveling wear levels all the data blocks, including the ones which are not written, unlike dynamic wear leveling. In the background, this is done transparently to the host system. Various providers have various mechanisms to trigger a static wear leveling.

For example, the difference between blocks in the static data pool and blocks in the free data pool could be one such case. When this threshold is enabled, the block in the lowest program / erase count static data pool is switched to the highest program / erase count block in the free data pool. (Cactus Technologies Wear Leveling-Static, Dynamic and Global, 2019).

Figure 15. Static Wear leveling Conceptual Implementation (Cactus Technologies Wear Leveling-Static, Dynamic and Global, 2019)

TRIM Functionality

The TRIM is the command that enables the operating system to notify the SSD that the next time it completes a block erase, it can skip the process of re-writing that particular data. Thanks to this command, the total number of data entered in the disk is less, thus raising the life of the SSD (there is another technique, called wear leveling, which we discussed earlier). All readings and writings harm the memory, but writing does much more damage than reads, the durability level of the block has luckily proven not to be an issue for new NAND flash memories. Trim is an ATA command used by the operating system when we delete a file. Also, this command offers us the path to

communicate between file-level and block-level, so that the operating systems can notify the SSD that the files are deleted, and the file pages are marked as stale.

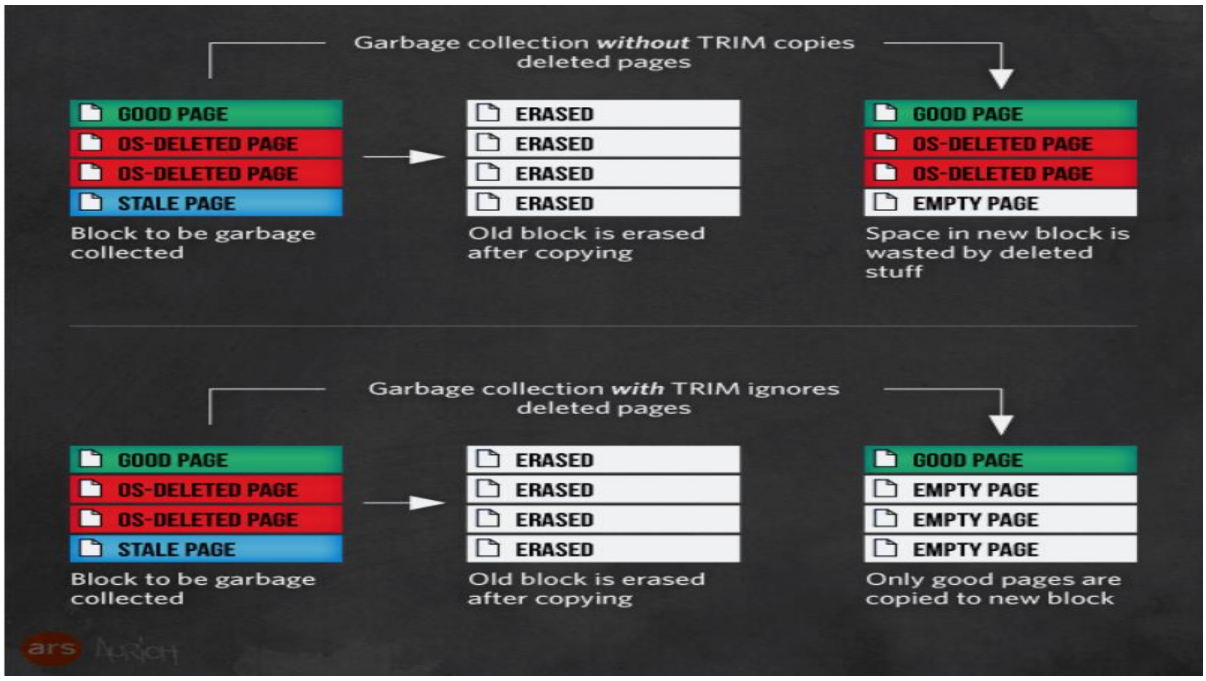

Figure 16. *TRIM with Garbage Collection* (Hutchinson, 2015)

The drive no longer has to save pages that belong to the deleted files with the help of TRIM. Trim does not rule out the need for garbage collection but works with garbage collection by making it easier to identify the marked pages as stale. Without the Trim, the garbage collection is not notified of the deleted files and pushes the pages containing deleted information together with the good pages, thereby raising the write amplification. Trim warns the controller that it can stop receiving pages with omitted content so that the rest of the block is left for deletion.

Trim adjusts the write amplification and increases the life and efficiency of the SSD.

Self-Corrosion

The mechanism in which retrievable elements are self-deleted or discarded over time, which are essential for completing the forensic tests, is called as self-corrosion. Regarding modern SSDs, it is a process in which the controller in the flash memory deletes the blocks marked as deleted, making it difficult for the forensic examiner to retrieve the block. The self-destructive proof mechanism is triggered by the operating system command TRIM on the SSD controller when the user deletes a file, formats a disk, or deletes a partition. The TRIM is fully integrated with partition and volume commands. This process involves formatting or clearing partitions; file system commands for shortening and compressing of files, and system restores operations. Therefore, the Self-corrosion technique in SSDs for recoverable data currently makes the forensic investigation even more difficult.

Today's SSDs self-destroy proof, through the "self-corrosion" method. Garbage collection, which acts as a background mechanism in most modern SSDs, can continuously remove data in a matter of time after it is selected for deletion. Transferring the disk to another computer or connecting it to a write blocking unit cannot stop garbage collection. The only way to prevent corrosion is by separating the disk controller from flash memory chips, which store the data and then directly access the chips through custom hardware.

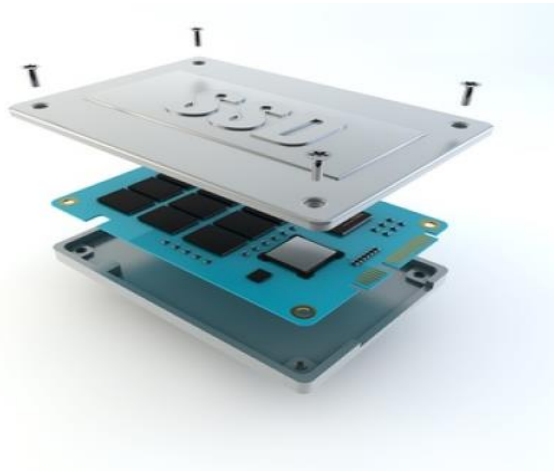

Figure 17. *SSD Hardware for self-Corrosion* (Gubanov, 2012)

Garbage Collection

Garbage Collection (GC) is an essential process with all solid-state drives (SSDs) but can be applied in various ways that affect the overall efficiency and durability of SSDs.

In comparison to HDDs, NAND's flash memory cannot re-write the existing data; it must first remove old data before writing new data at the same location. With SSDs, GC is the term for the process to move available data to new locations and to remove the invalid surrounding data. Flash memory is split into blocks, further separated into pages (Tokar, 2012).

Data is written to an empty page directly, but data can be removed if the block is full. Therefore, all the correct data from a single block must first be copied and written to the empty pages of a new block to retrieve the space used for invalid data. Only then can invalid data be removed from the original block so that new valid data can be written in this block.

One possible downside of the SSD is that while they can read and write data very quickly (mainly when the drive is unoccupied), the time for overwriting is much higher, and in this case,

it is slower. This occurs because when an SSD reads page-level data (from individual rows within the NAND storage grid) and writes on the same level, it only erases information at the block level, even though the nearby cells are empty!

It happens because the operation to remove data in the NAND flash requires a high voltage. We could remove NAND theoretically at the page level, but the total energy required to do so "harms" the cells which are surrounding to re-write our targeted data. This problem is reduced by data deletion at the block level. Also, only the SSD can update the previously existing block page by copying all the block's content to the memory, erasing the block, and then writing the old block's content with the updated page. If the drive is complete and there are no empty pages open, SSD scans blocks marked for deletion (that are not yet deleted), removes them, and then writes data to a newly deleted page. This is why an SSD becomes slower as it ages; a new and large empty drive has a lot of blocks available to write data instantly. In contrast, the rest of the drives are more likely to be forced to do the entire procedure (find and delete pages) and therefore become slower (Dimitrios, 2017).

Garbage Collection is the method that helps our drive to reduce the program / erase cycle output by introducing some tasks in the background. This process is shown below in the image.

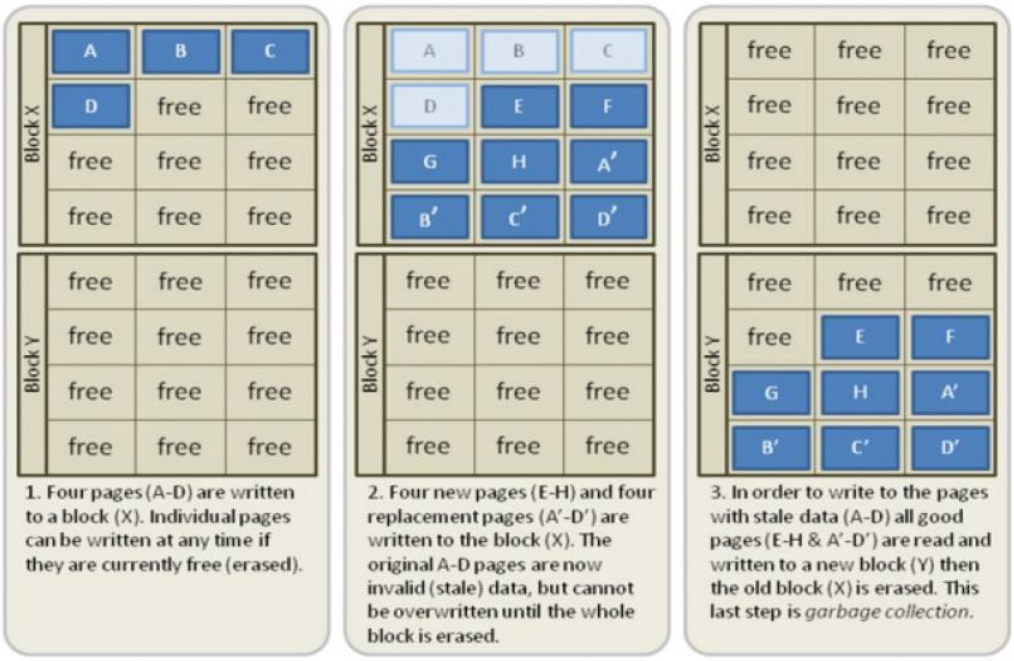

Figure 18. *Garbage Collection* (Dimitrios, 2017)

In this example, the drive takes advantage that it can write new values for its first four blocks very easily, which increases the write to the empty pages (A' to D'). Two new blocks, E and H, were also created. Now the blocks between A and D are labeled to be taken away by the garbage collector, which means that they contain data marked as old by the drive. The SSD moves its latest pages to a new block and deletes the old block and then marks it as free space. It gives the drive an advantage immediately; during the next time, it needs to write to the empty block X directly rather than executing the program / erase cycle faster.

Advanced SSDs run a complex process called garbage collection to avoid the undesirable impact of the aging of SSD. They do that because it is beneficial to keep as many empty blocks as possible ready to write. The process of garbage collection includes scanning the controller through the inventory of written pages, which are marked' stale' (i.e., changing the data they contain by the

OS). But since it's impossible to change the state of a page without first removing it, updates are made to new pages, and the old pages are inactive. The garbage collection searches for blocks with a mix of good and bad pages, and, as they replicate all the good pages into new blocks, it eventually eliminates and labels the old block ready to be used by the newer block.

Encryption

Encryption of hard disk drives applies a secret key or password mechanism that guarantees data security for computer hard drives. It protects the hard drive by securing each sector that also threatens the forensic investigation. Studies have shown how solid-state hard drives can mark deleted data from the flash memory page as invalid but not necessarily delete the page. And, if sensitive data is not always easily encrypted in the entire data process, it can also be retrieved as traditional hard drives. Highly qualified people can use encryption methods and external tools like BitLocker, TrueCrypt, PGP, etc. to achieve the highest degree of data security in SSDs. Such aspects would create more problems and complexities in the forensic investigation of SSD data analysis.

Therefore, due to the rapid growth of computerized crimes, such as intrusion, stealing of data, illegal acts, sophisticated hacks of governmental systems, digital forensics analysis, and research, growing technologies also need to advance in all fields. The precautionary collection and analysis in modern SSD's would require no harm to the device, and almost all the data missing from the system would be retrieved as substantial evidence at the trial. Up-to-date skills are required to extract critical data from modern SSDs, which is mandatory for computer safety professionals. A complete image of the SSD hard drive allows forensic examiners to obtain a hash value that could be used as proof in the Court in the course of any criminal investigation. However,

hard disk manufacturers typically build drives with extra storage, which are not accessible by traditional methods via the operating system. This demonstrates how the flash memory, the controller, TRIM functionality, self-corrosion, garbage collection wear leveling, encryption, and other modern SSD features make it harder for forensic examiners during an investigation (Joshi & Hubbard, 2016).

Summary

In this chapter, we discuss how important are SSDs and HDDs. We describe in detail the functioning of both drives. We also discuss the advantages and disadvantages of SSDs and HDDs; we compare them as well. The chapter also discusses how data is deleted and recovered in both the drives. It also focuses on concepts like wear-leveling, garbage collection, encryption, self-corrosion, TRIM functionality, which complicates the forensic investigation.

Chapter III: Methodology

Introduction

The Solid State Drives, which use flash memory (such as DRAM or SRAM), have suppressed the traditional Hard drives which use spinning platters to read and write data by becoming the primary storage units on laptops. The new generation gadgets like smartphones, tablets, and notebooks would not have come into exitance without flash memory or Solid-state drives. As we already know from the previous chapter that SSDs do not have moving parts like turning plates or versatile read/write heads, which have been used in conventional hard drives or floppy disks. While traditional Hard disks are usually a pile of magnetic materialled disks that store data in terms of '0' and '1', which is an added advantage for HDDs because they cannot write in the same location every time. So basically, when information is erased, that part would be recorded as deleted, but those erased files would be accessible for us to recover at any point in time, which are usually placed in an unused sector. But considering today's situation with advancing modern studies and technological performances, the SSDs which are used in day to day lives are not able to empty the sectors in the drive, thus causing a new problem to recover deleted files. The invalid files are deleted by the TRIM functionality, and that will also take care of the rewrite functionality. This mechanism may end up deleting valid files as a result of false positives, which may be very crucial for a case in forensics. Improving the functionality of the TRIM command can increase our possibilities of getting better results and have a better chance of solving the case. To do that, we proceed further to understand SSDs in-depth and perform the TRIM functionality on multiple SSDs and analyze their results. We would also understand how the concepts of garbage collection, wear leveling, self- corrosion, and encryption work on them.

Further, we will discuss the possibilities of having better solutions to achieve better results for acquiring as much as valid data to support digital evidence.

Design of the study

A windows operating system is needed, which runs on an SSD. The experiment's primary purpose is to evaluate the TRIM behavior, so we try to obtain an operating system that is calibrated to Windows 7 or higher. All operating systems in Windows 7 and above have a built-in TRIM command which the user may change. So, we're trying to test the TRIM command, and we'll make sure it's activated on the OS. The full SSD is formatted and loaded with files and documents on which we want to experiment. Initially, these files are loaded when TRIM is disabled. We then delete a few files and then add a new set of files. Now, we use a Forensic tool kit Imager to build the disk image and scan the keywords through the files. For the analysis, the results obtained during the TRIM command are used as assumptions for the study. When the tests have been collected, the administrator enables the trim command on the operating system. Now, we delete few files from the already existing files and add new files when the trim is enabled, and the same procedure is performed for creating the image in FTK Imager. The result is compared with each other, and this helps us to evaluate the TRIM command status on the Solid-Drives in the forensic investigations to retrieve evidence.

Data Collection

The process uses two laptops, one is Lenovo yoga 720 with Intel® Core™ i5-7^{200u} CPU @ 2.50GHz, 256 GB Solid State Drive, and 8.00GB RAM and the other laptop is HP AMD A9-Series-4 GB Memory-AMD Radeon R5 Graphics-128GB Solid State Drive. We load images, word documents, excel sheets, etc. The laptops which we are using are run on windows 10 operating

systems. An External SSD of 120GB is used for this experiment. It is connected with a SATA 3.0" cable. Trim is enabled and disabled on the operating system, and images are created with FTK imager. Files are deleted and added before creating the image for both the SSDs, i.e., Internal and External SSDs.

Tools and Techniques

Hardware and software requirements

- Laptop- Lenovo yoga 720 i5-7TH Gen
- Windows Operating System
- FTK Imager
- Autopsy
- Microsoft Office

Test Devices

- PNY Solid State Drive 120GB 2.5" SATA
- HP Laptop Internal SSD 128GB

Figure 19. a) Lenovo Yoga 720 i5-7Th Gen connected to External SSD

b) Solid State Drive Laptop

Figure 20. PNY Solid State Drive 120GB 2.5” SATA

Figure 21. HP Laptop Internal SSD 128GB

Literature Related to Methodology

How does TRIM SSD work?

To learn the functionality of TRIM, users should know how the SSDs work. The basic unit used to read and write data on SSD is ' page, 'and 128 pages form a data block together. Once a command is given to remove any data, SSD initially deletes the entire block holding the appropriate page and copies the data to another block. Instead, except for the deleted portion, it restores all other pages to the block back (Belkasoft, 2014).

TRIM command allows the Windows Operating System to communicate about what data page needs to be removed from the SSD. In this case, SSD need not remove and restore a whole block.

It can only delete the specified page effortlessly. Therefore, the SSD drive controller is more effective in handling usable storage space. It's all about SSDs TRIM feature running in Windows 10, 8, 7, versions.

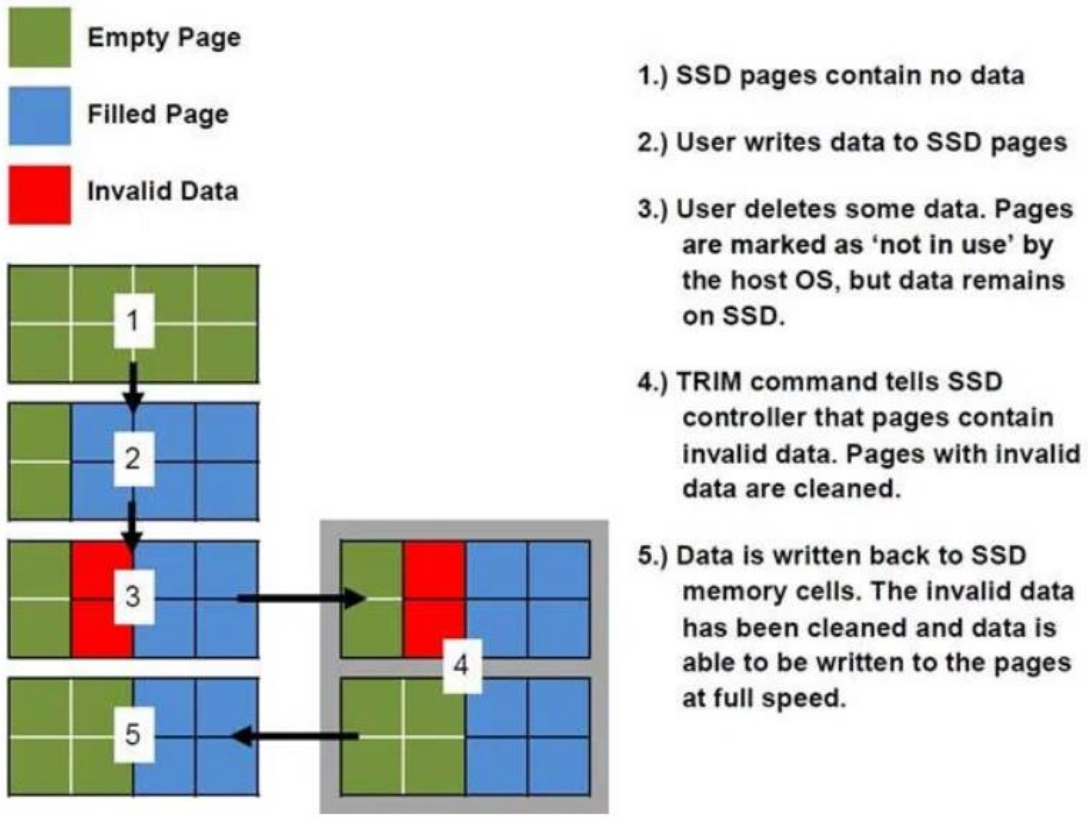

Figure 22. *TRIM working on SSD* (Belkasoft, 2014)

Enabling TRIM for SSDs in Windows Operating System

With TRIM allowed, SSD drives do not delete the whole data block but delete only the required page. Thus, TRIM increases the writing speed of data on SSD drives substantially. It also increases an SSD drive's total life span.

How to Check for TRIM status on SSD?

The TRIM feature should be available if we are using Windows 7, 8, 10, and have an SSD drive connected to the device. However, we can always test whether the TRIM feature is allowed or not. Here is how we can test whether the TRIM function is allowed in SSD:

Step 1: –First, by typing cmd in the search box, open a (CMD) command prompt on the device.

Step 2: –In the command prompt type "*fsutil behavior query DisableDeleteNotify*" and click enter

Step 3: –One of the results is displayed on the command prompt: "*NTFS DisableDeleteNotify= 0"* –This result means TRIM is allowed.

"*NTFS DisableDeleteNotify= 1"*–This result means TRIM is disabled (Arora, 2019).

How to enable TRIM for SSD?

To enable TRIM open command prompt and type in "*fsutil behavior set disabledeletenotify 0,*" then click on enter, the TRIM will be enabled with the following message *"NTFS DisableDeleteNotify = 0."*

How to disable TRIM for SSD?

To disable TRIM type, "*fsutil behavior set disabledeletenotify 1*" in command prompt. TRIM will be disabled with the following message on the screen "NTFS DisableDeleteNotify = 1."

Summary

In chapter, we discuss how SSDs are not able to retrieve data. To overcome this flaw in SSDs we perform an experiment when TRIM is enabled and disabled to extract the evidence files.

Chapter IV: Data Presentation and Analysis

Introduction

In this chapter, we explain how the data was gathered by acquiring both internal SSD and external SSD images. We will analyze how to use the trim feature and how it works effectively. By modifying the trim command, we'll explore how data is collected and deleted from the drives. In the next chapter, we explore the performed comparison and analysis of the extracted data from the acquired images, along with the results obtained from both the drives. The tools used for this process are FTK imager and autopsy.

Data Presentation

The data collected during this process contains pictures, pdf files, documents, and various other files. Different files used for performing the forensic investigation are in all the drives.

External SSD

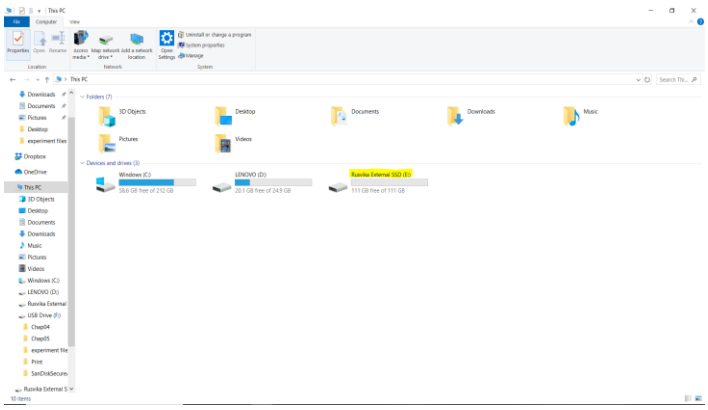

Figure 23. External Solid-State Drive connected to Laptop

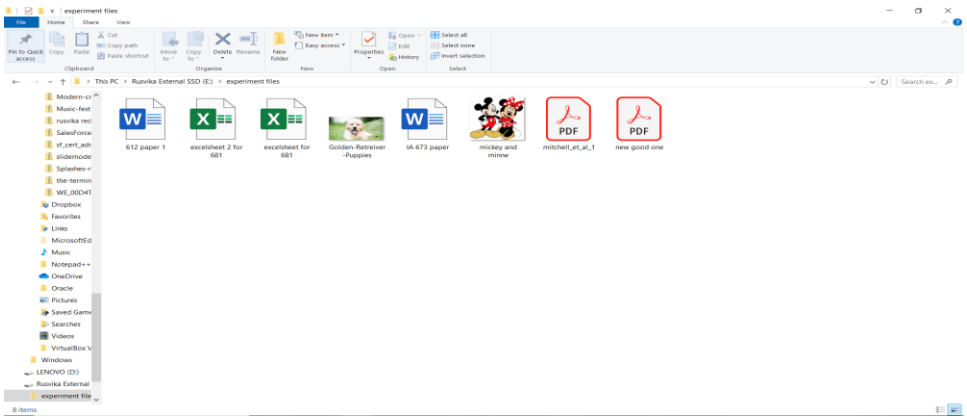

Figure 24. Before deleting files from External SSD

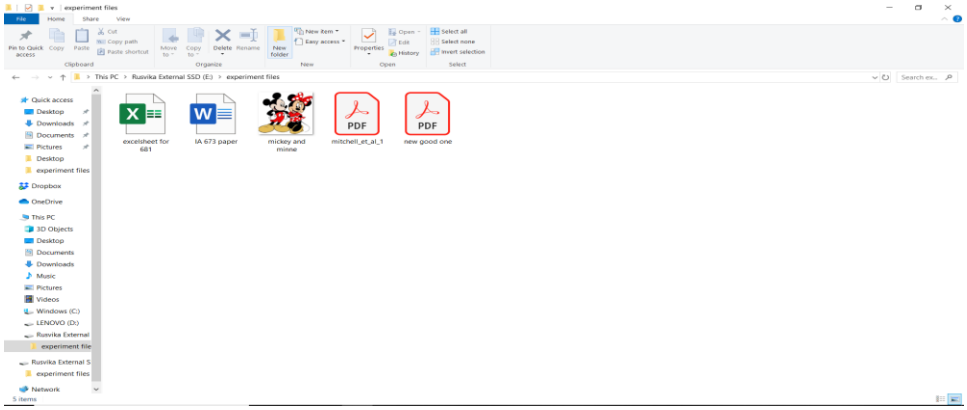

Figure 25. After deleting files from External SSD

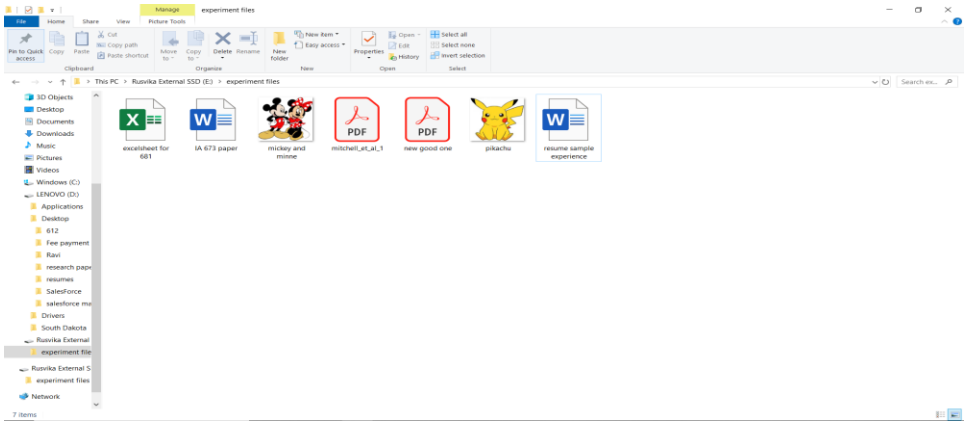

Figure 26. After adding new files to External SSD

Here, after we enable Trim, we delete the files and then add new files to the external SSD.

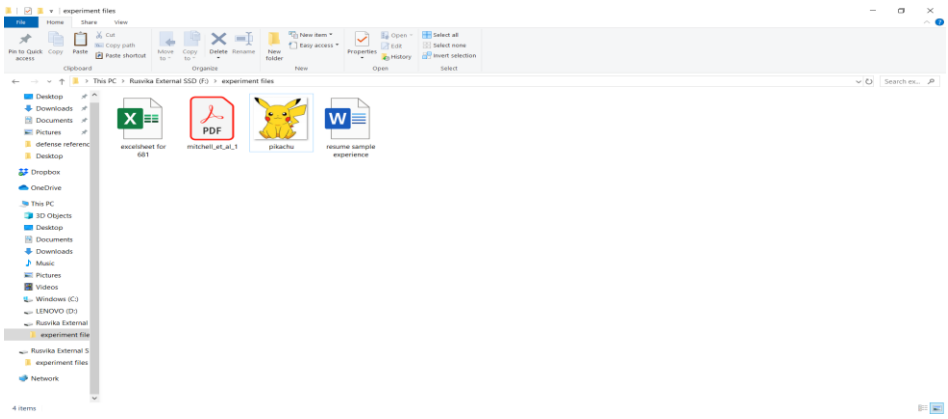

Figure 27. Trim is enabled, and files are deleted

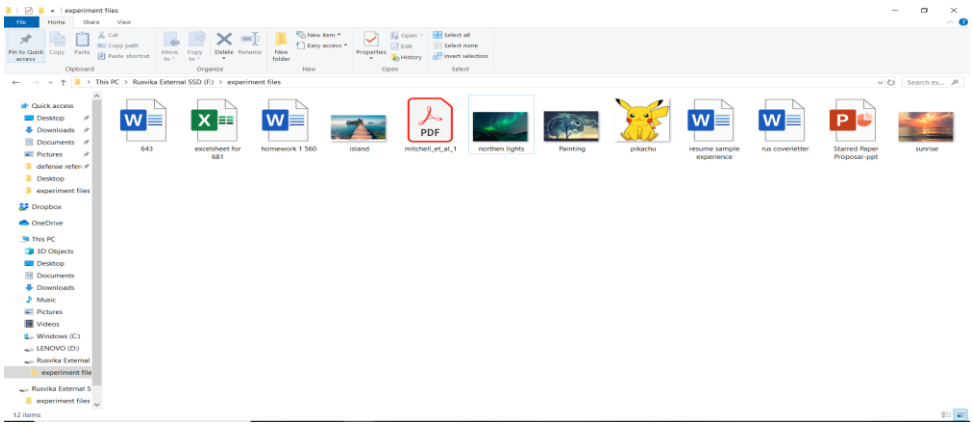

Figure 28. After that, we add new files to the external SSD when Trim is enabled

Internal SSD

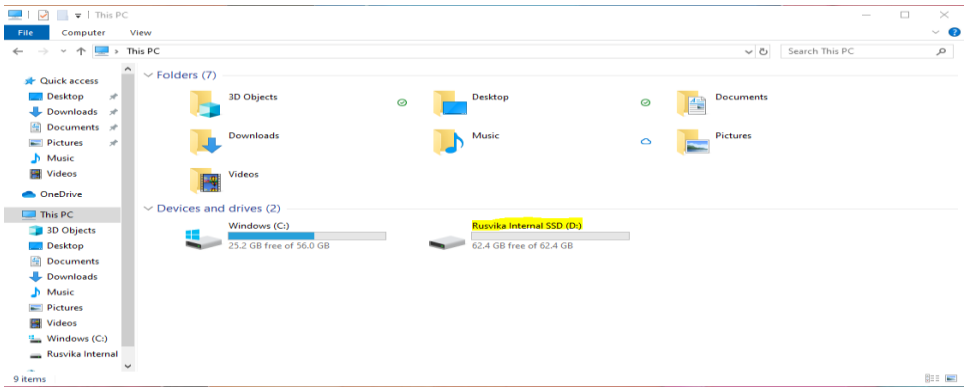

Figure 29. Internal SSD drive in the laptop

We have the same set of files in internal SSD as well.

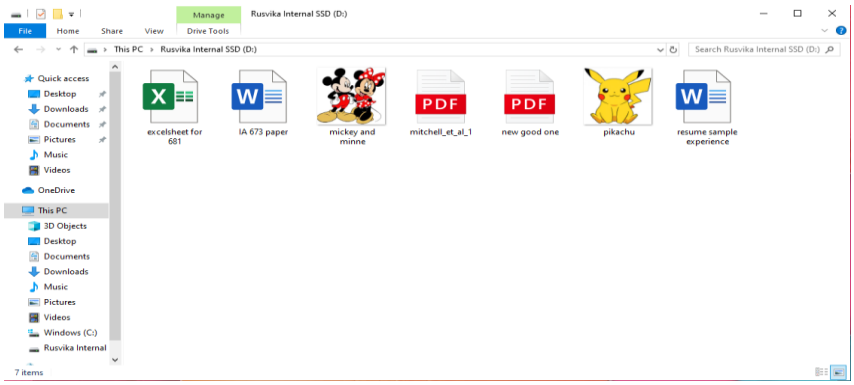

Figure 30. After deleting and adding new files to Internal SSD

We follow the same process which we used in external SSD, i.e., enabling Trim command and deleting the files and adding new files to the drive.

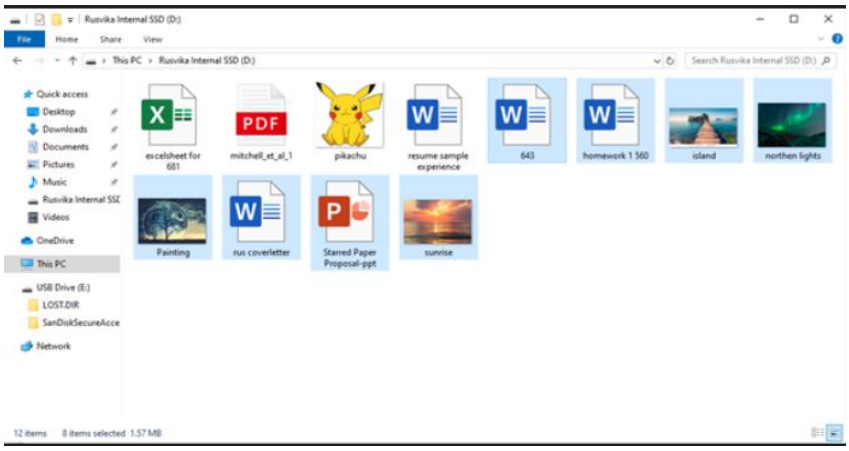

Figure 31. After we add new files to the Internal SSD when Trim is enabled

Installation of FTK Imager

- Download FTK imager with the following link.

  https://accessdata.com/product-download/ftk-imager-version-4-2-1

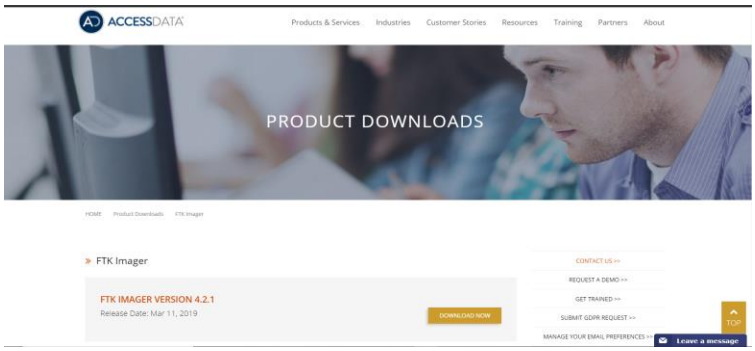

Figure 32. FTK Imager webpage

- To get the link for downloading, we must fill in the details.

Figure 33. Form for downloading FTK Imager 4.2.1

- We get the confirmation email along with the link sent by Access data.

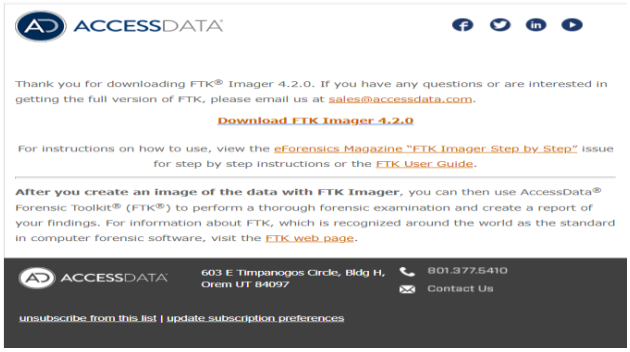

Figure 34. Download link sent to the email

- Steps for installation after downloading the FTK.exe file are as below.

Figure 35. License for FTK imager while downloading

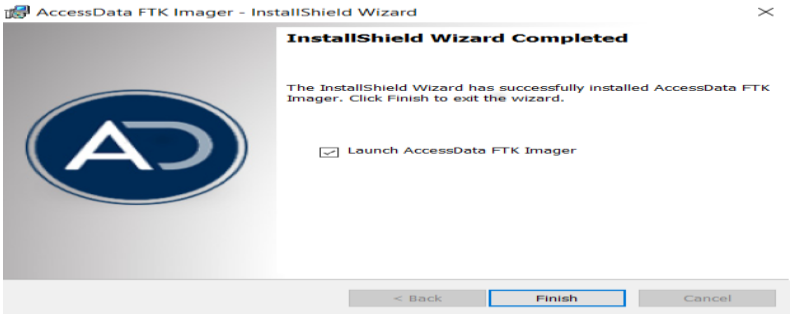

Figure 36. Installation completed window

- We launch the FTK imager after it is installed.

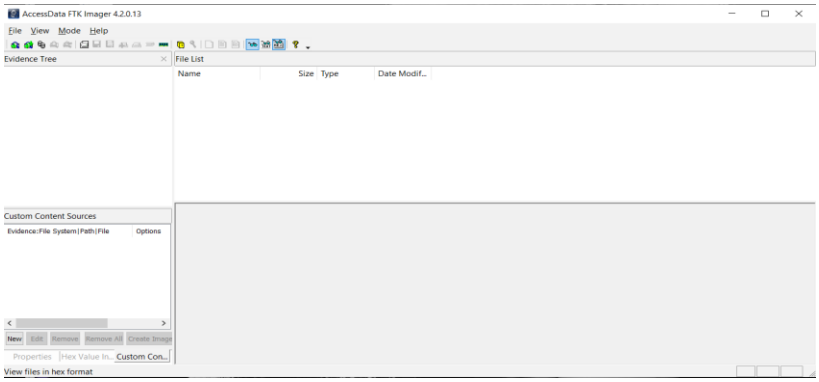

Figure 37. FTK Imager User Interface

Creating Image of External SSD

Before we create an image for external SSD, we check for the TRIM status. We create two images, i.e. when Trim is disabled and enabled**.**

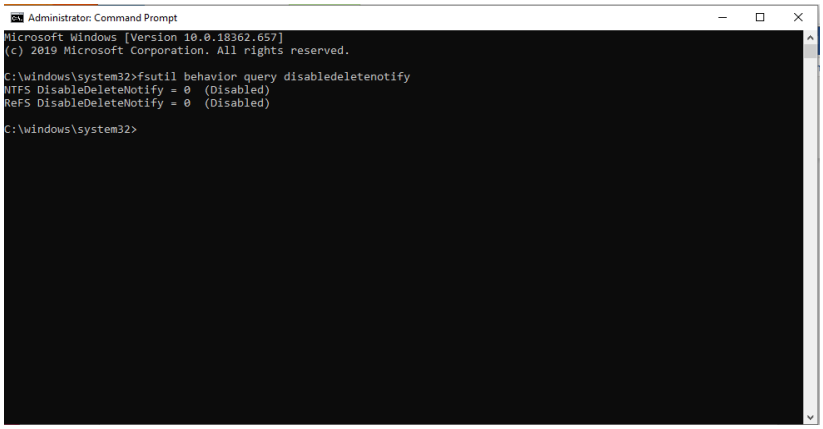

Figure 38. Checking what state TRIM is in

TRIM Disabled for External SSD

Firstly, we create an image when TRIM is disabled.

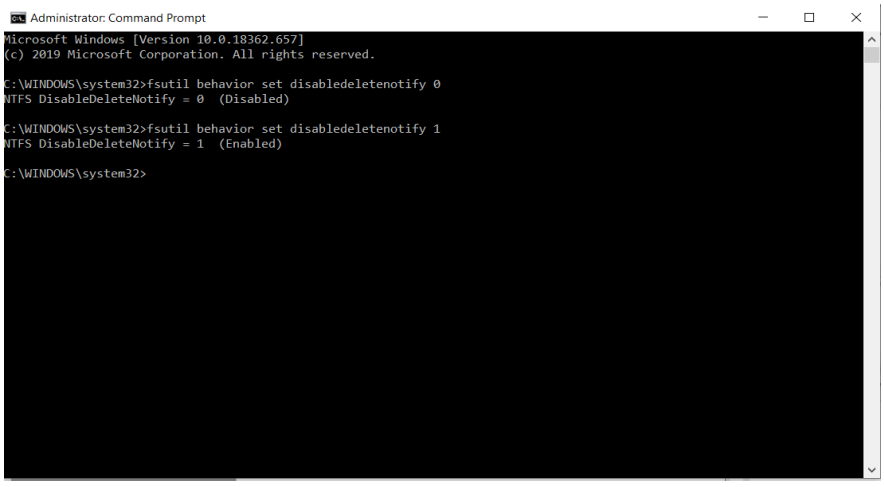

Figure 39. TRIM is disabled in command prompt

Here, we select the file and create a disk image.

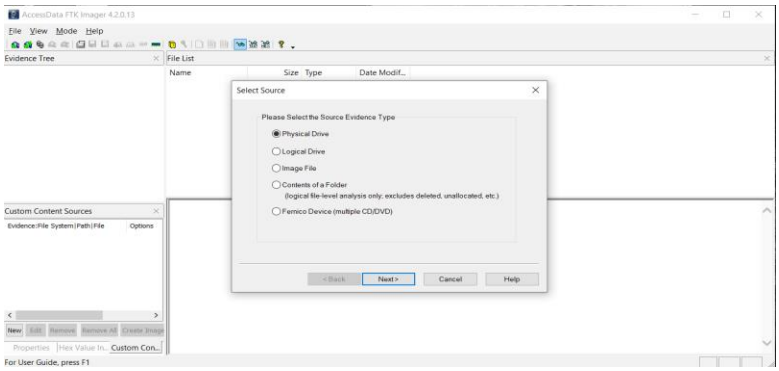

Figure 40. Source selection for evidence type in FTK Imager

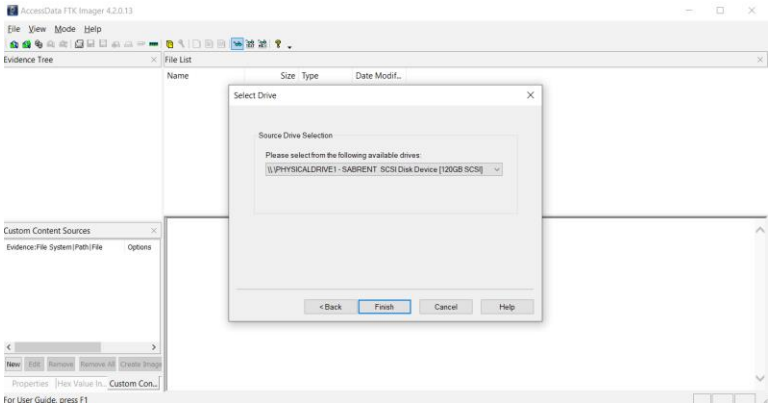

Figure 41. Selecting source Drive in FTK Imager

Evidence information is given for creating an image.

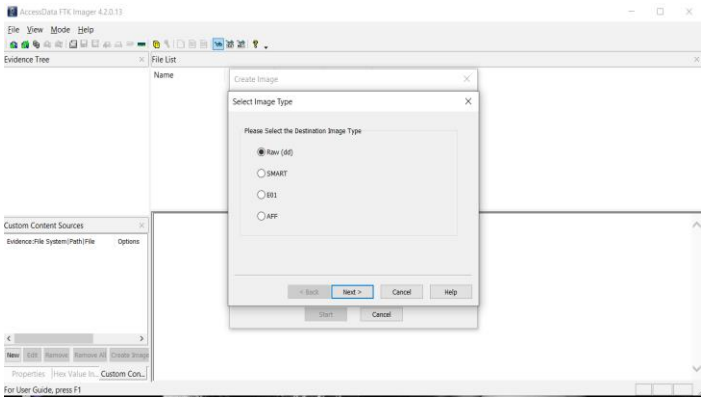

Figure 42. Image Type Selection

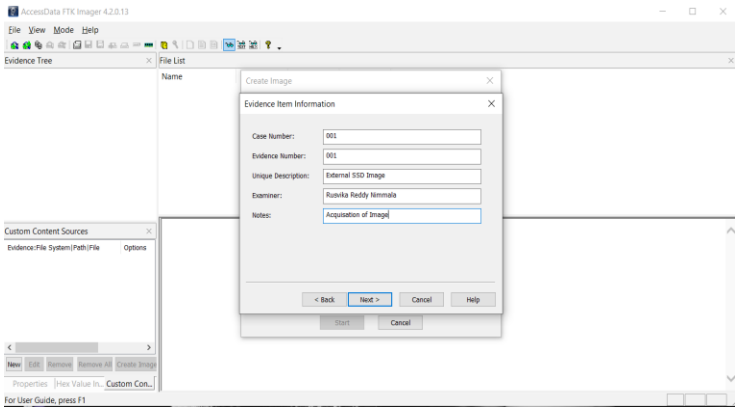

Figure 43. Filling up the Source drive Information

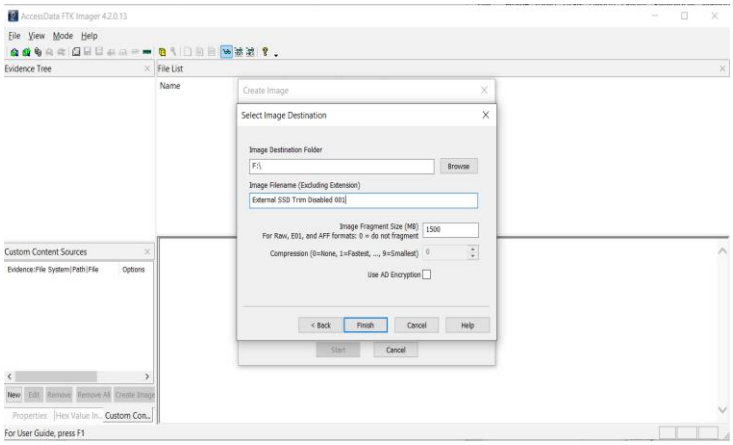

Figure 44. Selection of Image Destination

Below is the image creation process

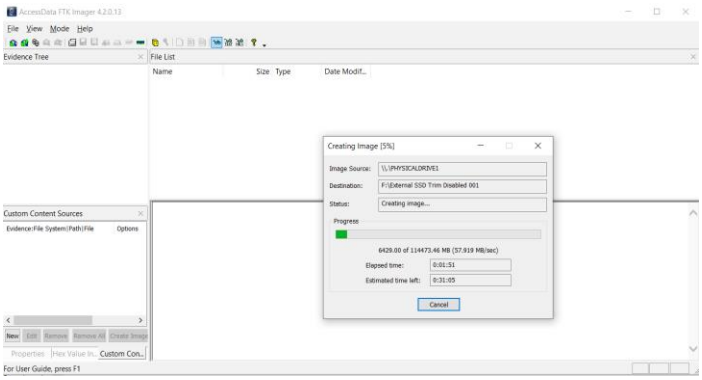

Figure 45. Image creation Started

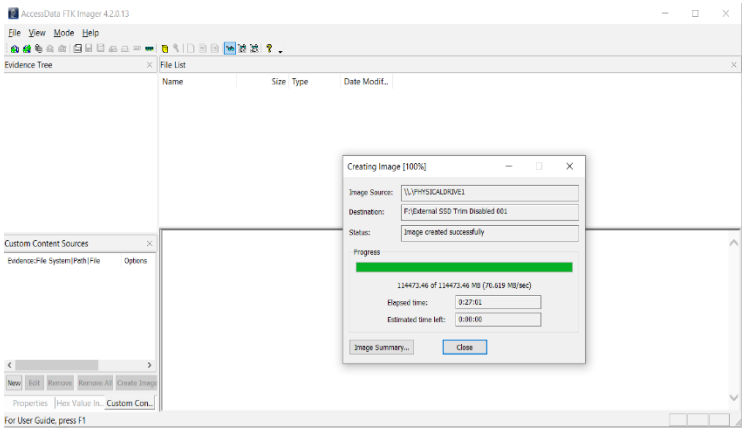

Figure 46. Image is created

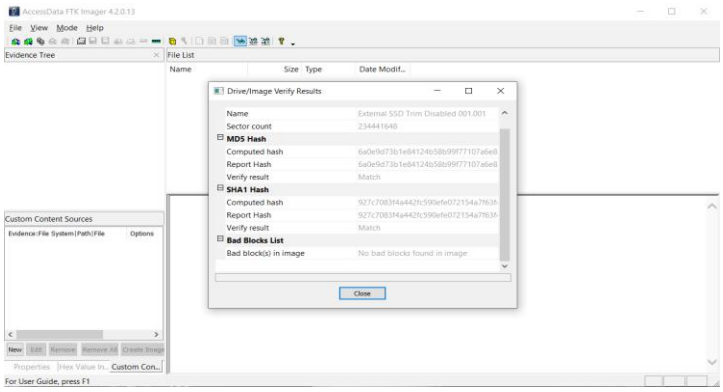

Figure 47. Verifying Hash values after the image is created

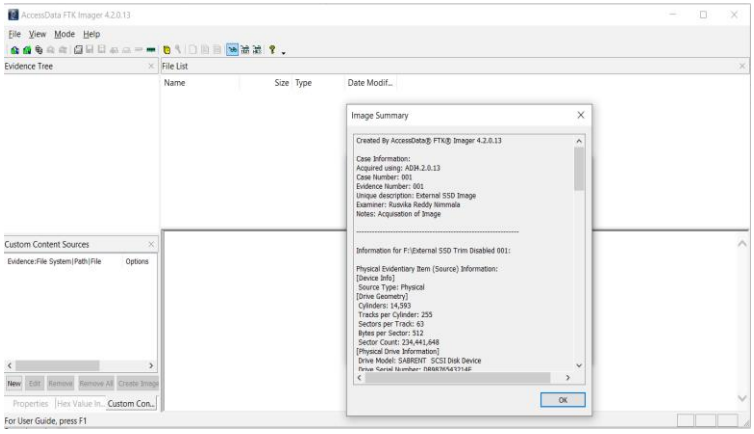

Figure 48. Image Summary is displayed

Similarly, we follow the same process for image creation when TRIM is enabled.

TRIM Enabled for External SSD

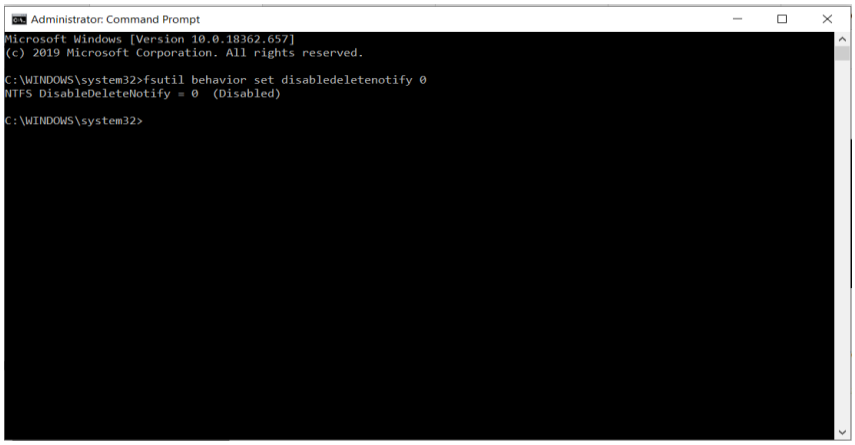

Figure 49. Setting TRIM status to 0

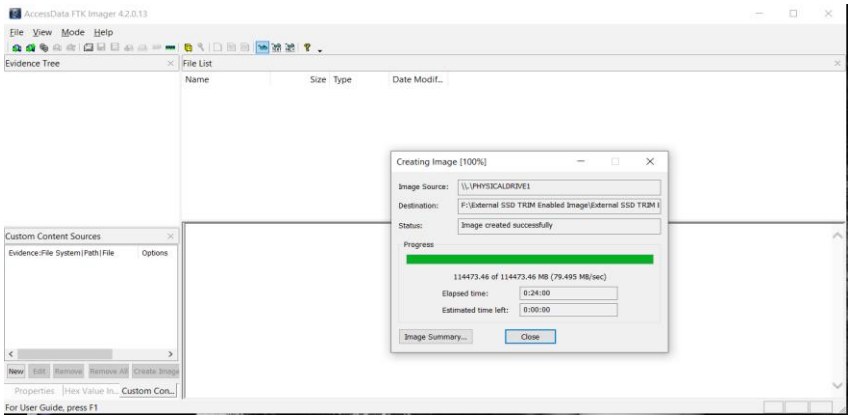

Figure 50. Final output when the image is created

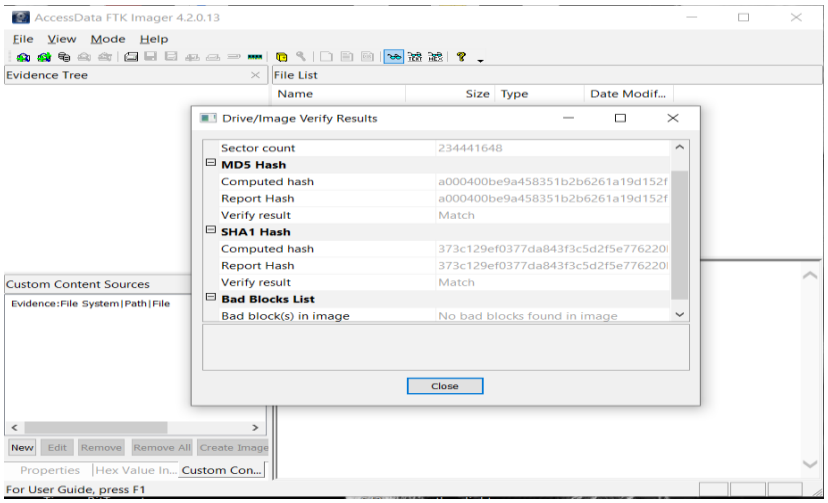

Figure 51. Verifying hash values when the image is created for TRIM Enabled in External SSD

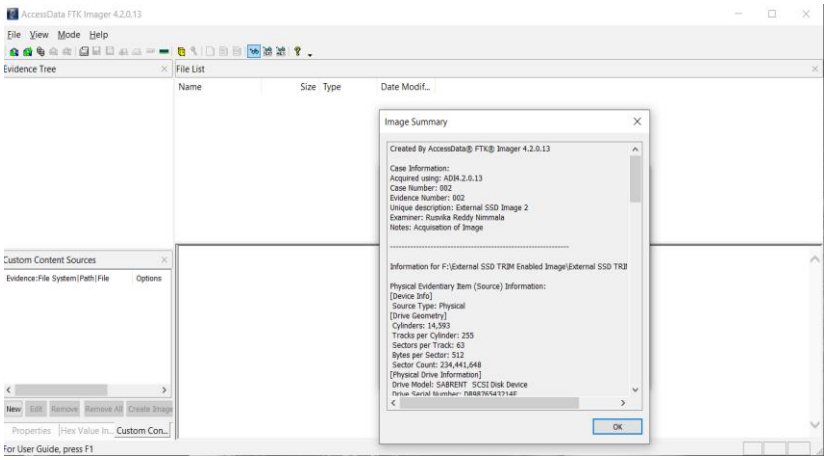

Figure 52. Image creation Summary

Creating Image of Internal SSD

TRIM Disabled for Internal SSD

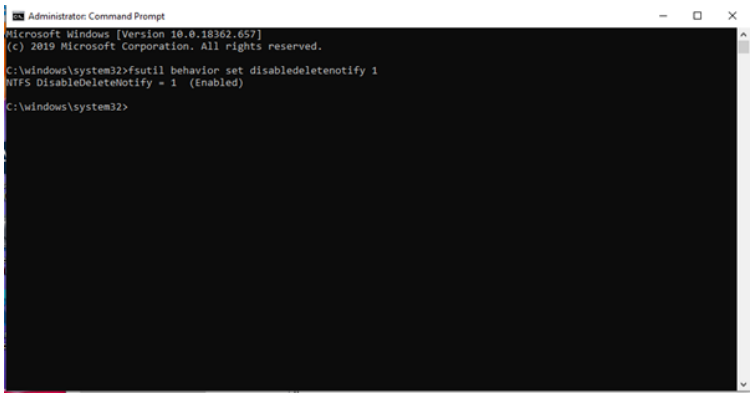

Figure 53. Set TRIM=1

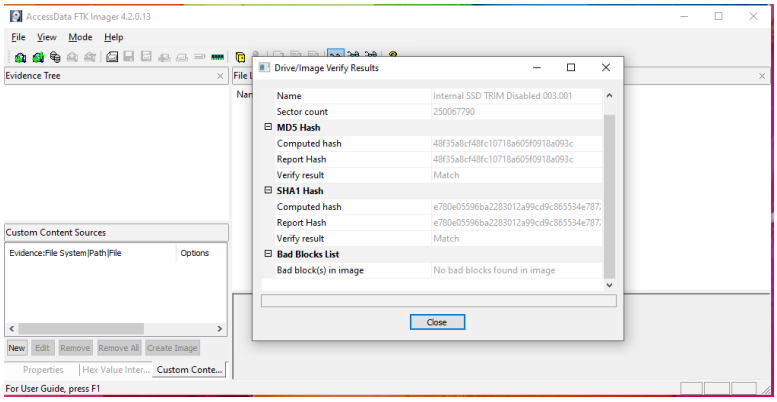

Figure 54. Verifying hash values for Internal SSD when TRIM is disabled

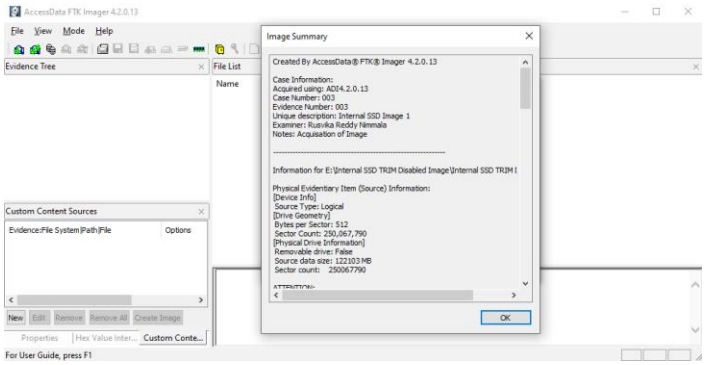

Figure 55. Image Summary for Internal SSD when TRIM is disabled

TRIM Enabled for Internal SSD

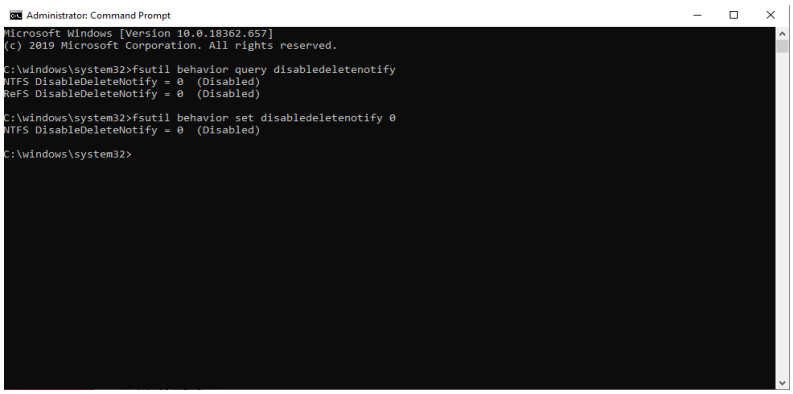

Figure 56. Set TRIM=0

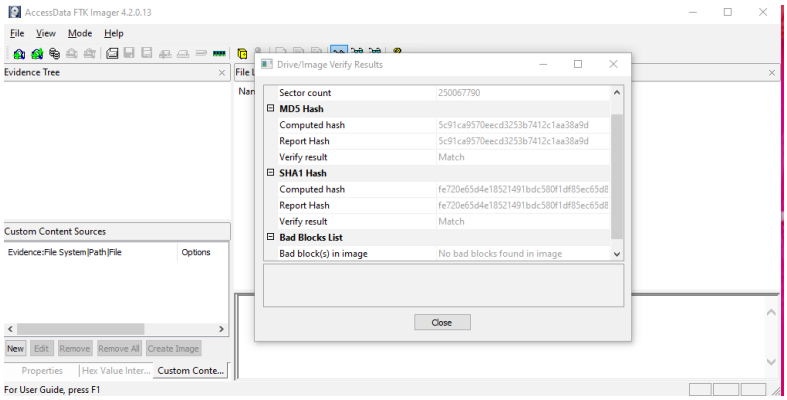

Figure 57. Hash value verification when TRIM is enabled in Internal SSD

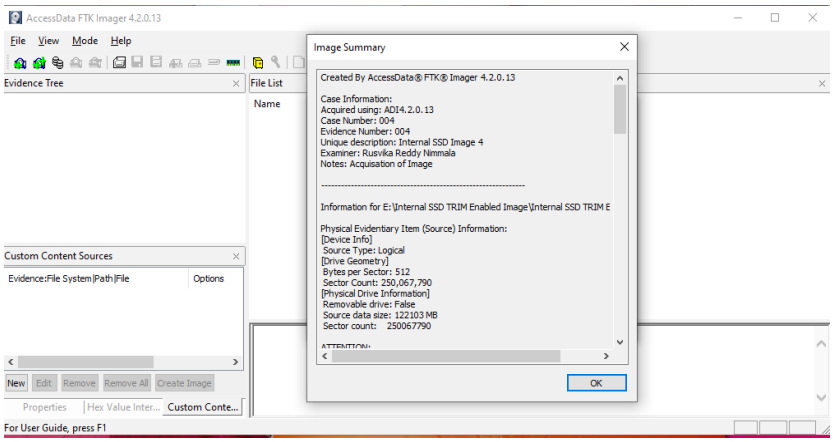

Figure 58. Image summary for Internal SSD when TRIM is enabled

Installation of Autopsy

Autopsy scans the internal and external SSD to recover deleted images, documents, excels sheets, etc.

Below are the steps for the installation of an Autopsy forensic tool kit.

- Download Autopsy from the following link https://www.autopsy.com/download/.

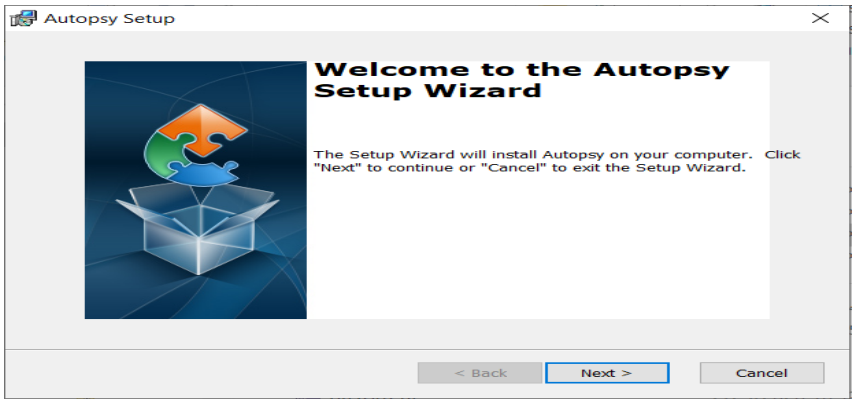

Figure 59. Autopsy setup wizard

- When you click next, it asks to select a folder where the tool should be downloaded.

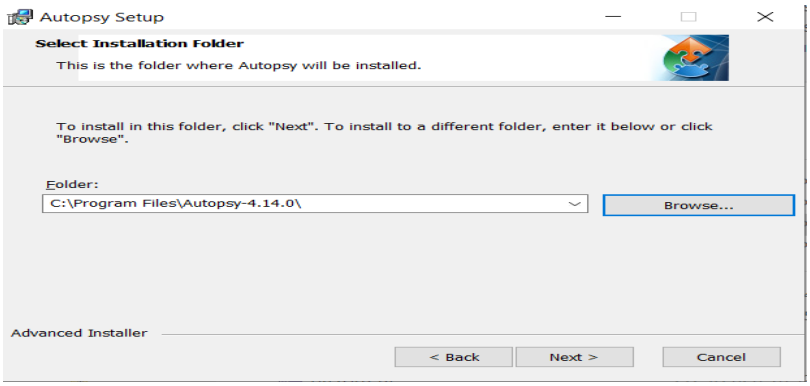

Figure 60. Selection of Installation folder

- After selecting the folder, click on next, then a new window opens where we have to select Install and change any installations if we want to.

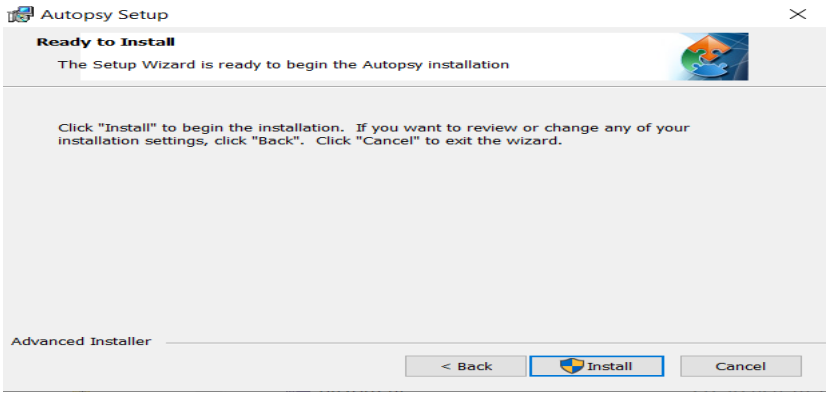

Figure 61. Installation setup window

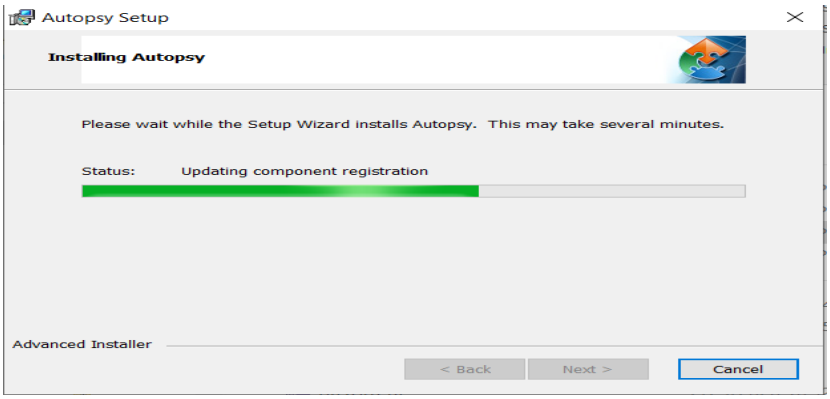

Figure 62. In-progress installation of Autopsy

Data Analysis

In the earlier section, the image is created with the help of an FTK imager. Now, we use Autopsy to analyze the image which we created.

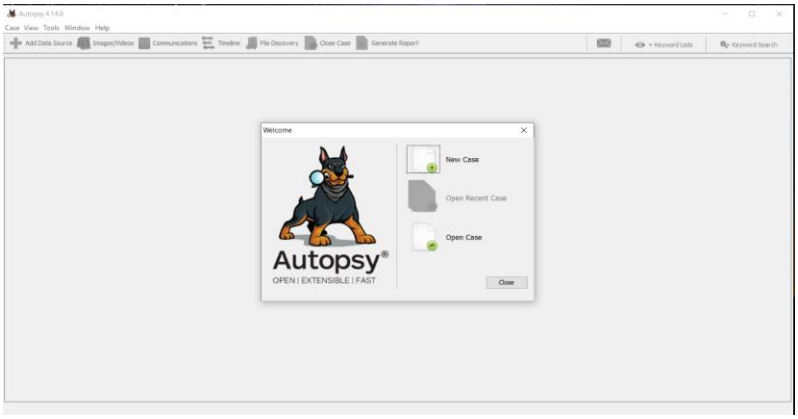

Figure 63. User Interface of Autopsy

Image Analysis for External SSD when Trim is Disabled

We start analyzing by selecting a new case; then, in the next window, we are asked to provide case information such as Case name and Base directory where the data would be saved. We should also provide information such as Case number, which is a unique number assigned to a case, Name, Email, Phone number, and other basic details of the Examiner. We should also write notes about the case if necessary.

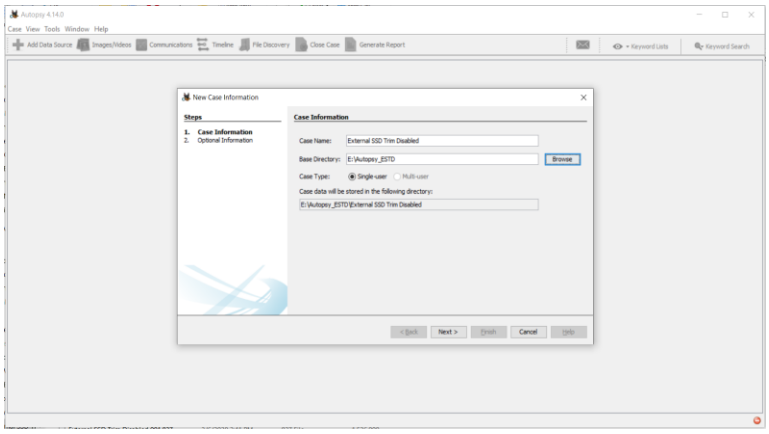

Figure 64. New Case Information window for Image 1

Next, we select what type of data source we have, such as disk image or VM file/local disk/logical file/unallocated space image file/autopsy logical imager results/XRY test export. In this step, we add the created image from the FTK imager.

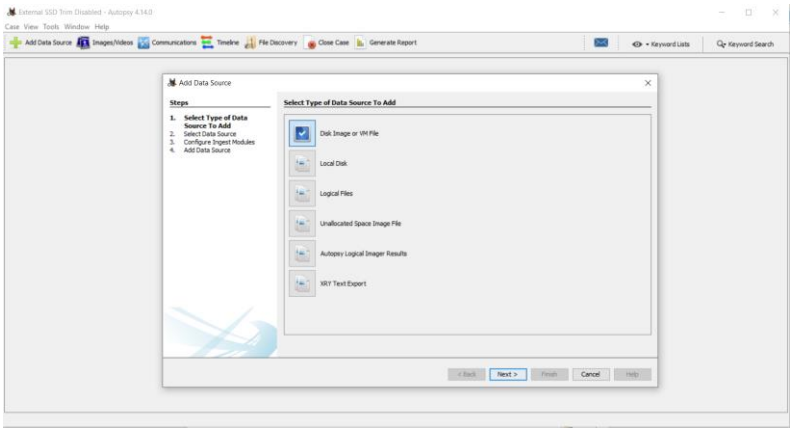

Figure 65. Selecting Image type

Now, we choose the image location.

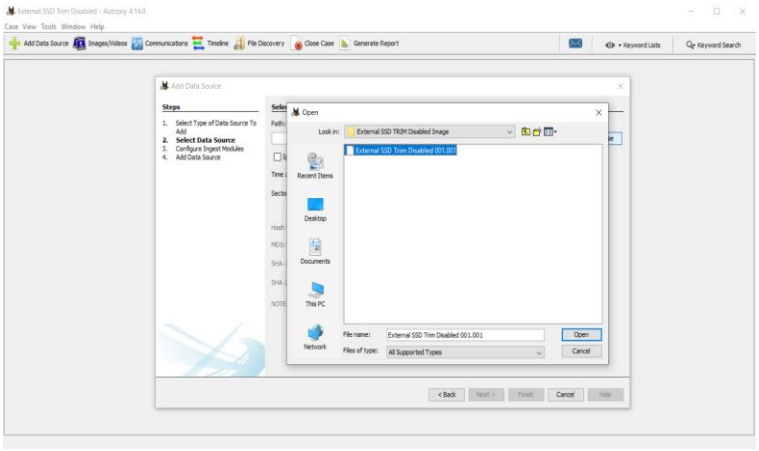

Figure 66. Location of the acquired image

In the next window, we select options that we consider during a forensic investigation. We check the fields to get information about errors and events.

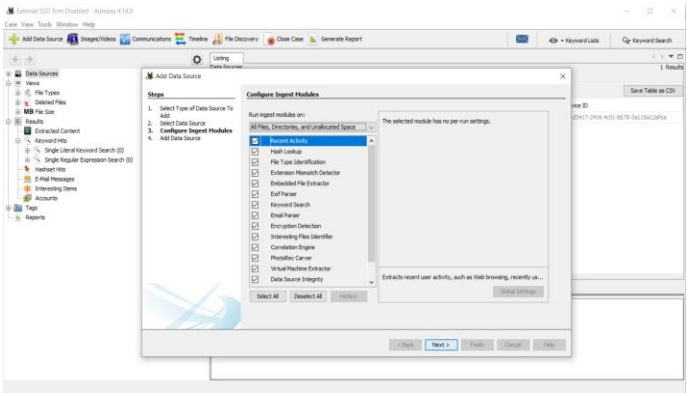

Figure 67. Configure Modules to perform

We add the data source and click on the finish, and the autopsy will start analyzing the image.

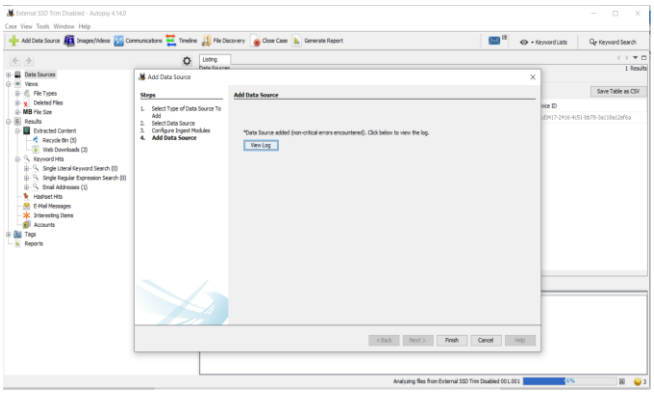

Figure 68. Adding Data Source and analyzing the data source

After data analysis is done, the next step is to analyze data source integrity.

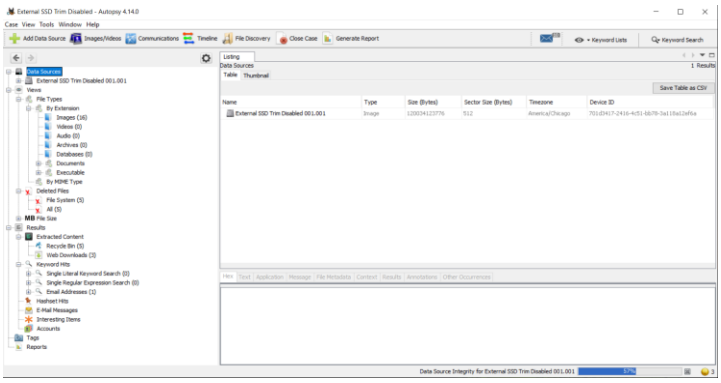

Figure 69. In-Progress setup of data source integrity

Results of External SSD when Trim is Disabled

To analyze the image, the time taken was approximately four to five hours.

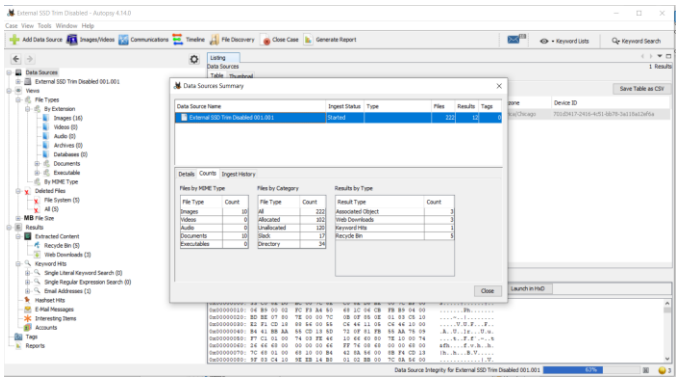

Figure 70. Count of files by category and mime-type

We search for files that are deleted.

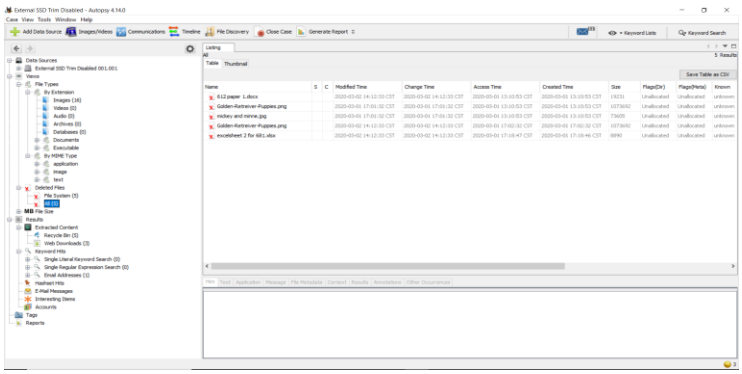

Figure 71. Files found in recycle bin

In the keyword search box, we search for indexed words. In the below figure, we searched for "*612 paper 1*, *excel sheet 2*, *puppies*" and got the keyword hits for the First Image.

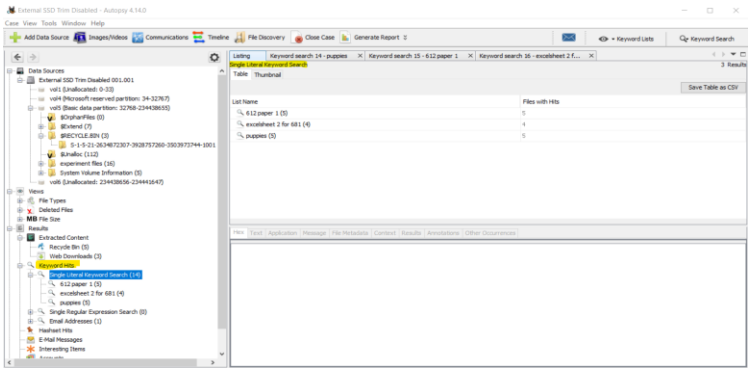

Figure 72. File hits for *612 paper 1*, *excel sheet 2*, *puppies* for image 1

Below is the Autopsy forensic report for First Image.

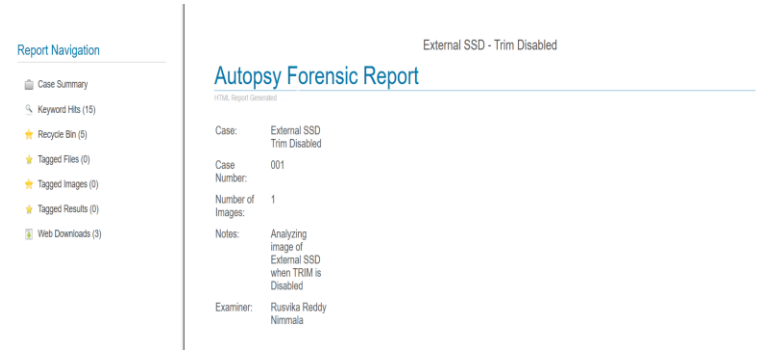

Figure 73. Autopsy forensic report for External SSD TRIM disabled

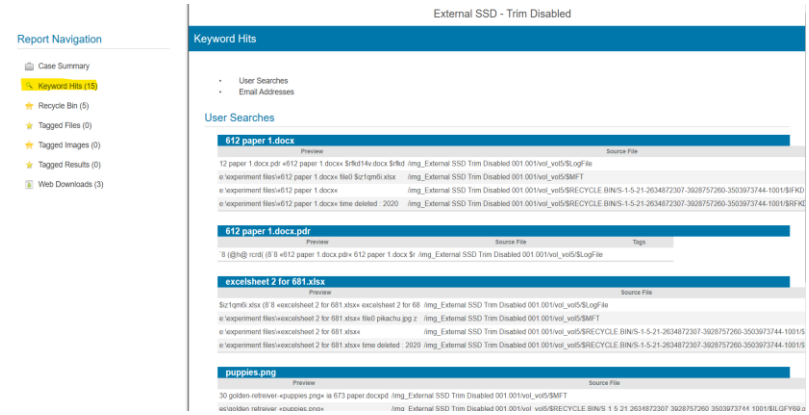

Figure 74. Keyword Hits for Image 1

Figure 75. Searches of web downloads

Image Analysis for External SSD when TRIM is Enabled

We provide details such as case number, examiner name, email, phone number, and notes for the second image.

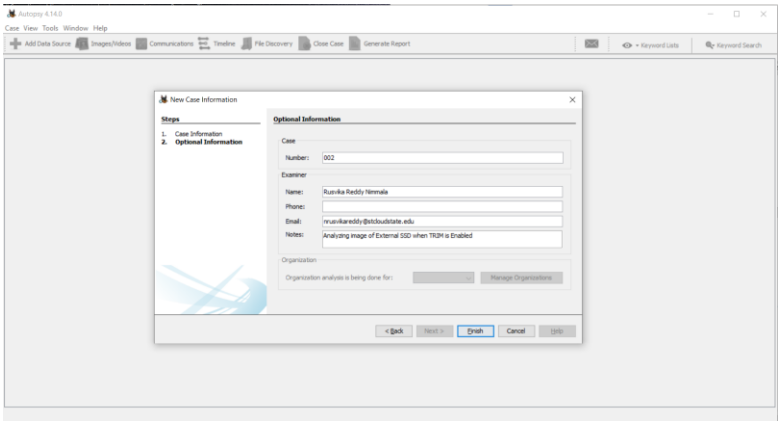

Figure 76. New Case is created for Image 2

We select what modules should be performed during the analysis.

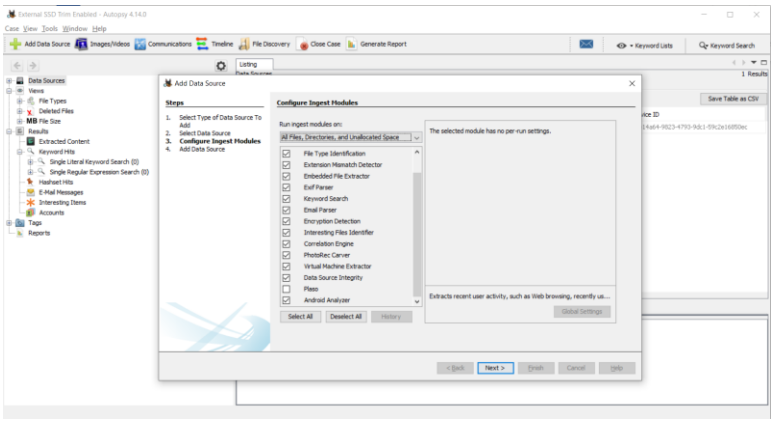

Figure 77. Configure modules for Second Image

Results of External SSD when Trim is Enabled

When we click on the data source summary, we get the count of files by mime type and files by category. The count is also displayed by the result type.

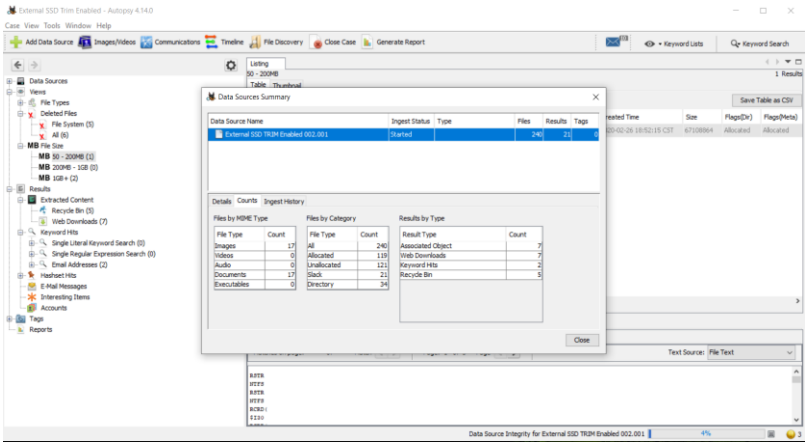

Figure 78. Data Source summary for the Second image

In the keyword search box, we search for indexed words. In the below figure, we searched for "*673, mickey and minne, new good one*" and got the keyword hits for the Second Image.

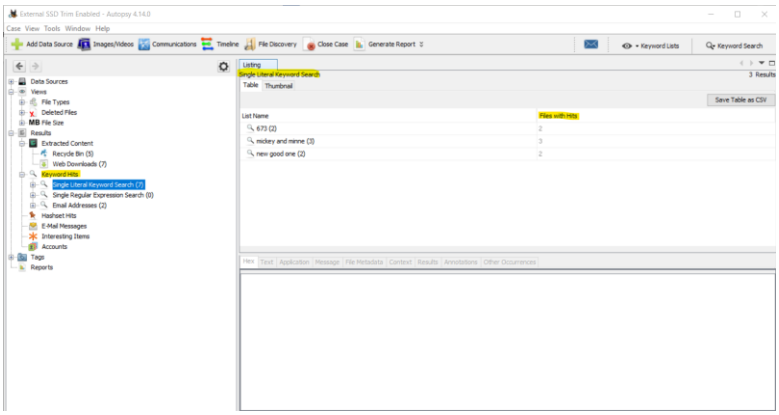

Figure 79. File hits for *673, mickey and minne, a new good one* for Second Image

Below is the Autopsy forensic report for Second Image.

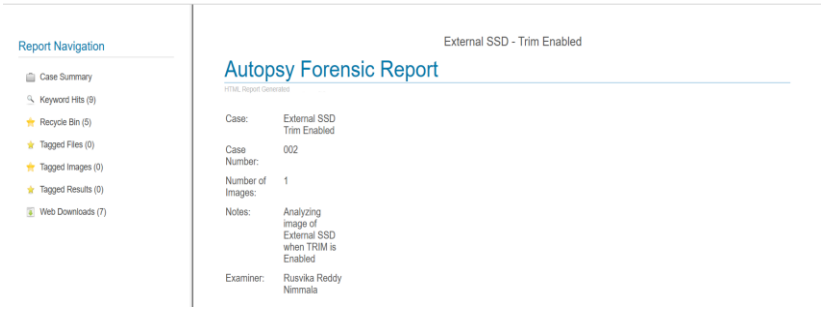

Figure 80. Autopsy forensic report for External SSD TRIM enabled

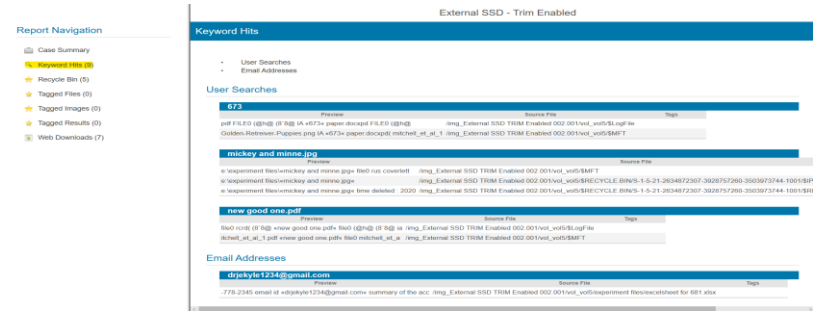

Figure 81. Keyword Hits for Image 2

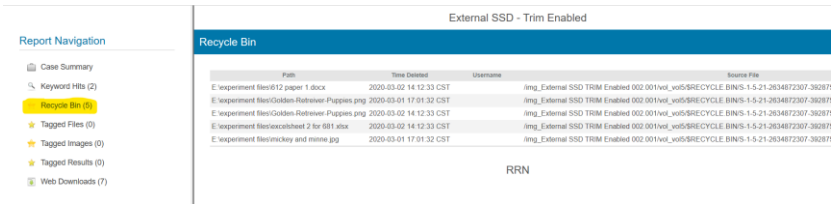

Figure 82. Search results of Recycle Bin Files

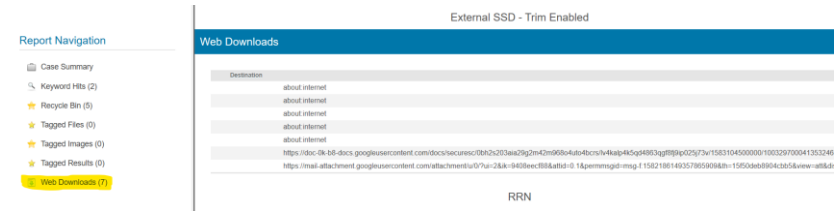

Figure 83. Search results of Web downloads

Image Analysis for Internal SSD when TRIM is Disabled

Now we analyze the third image. We give the directory name where we want the image data to be stored.

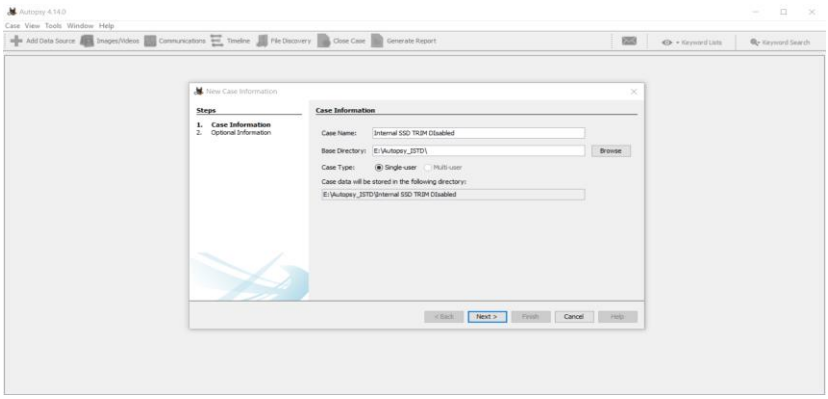

Figure 84. Case information for the Third Image

We fill in information such as case number, examiner name, email, phone number, and notes for the Third image.

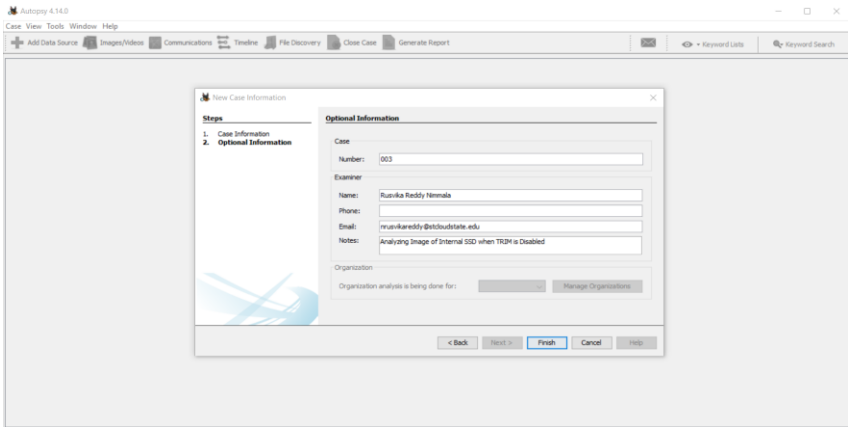

Figure 85. New Case is created for Image 3

Results of Internal SSD when Trim is Disabled

After the analysis is done for the third image, we check for the results in a data source summary where we can find files by category, files by mime type.

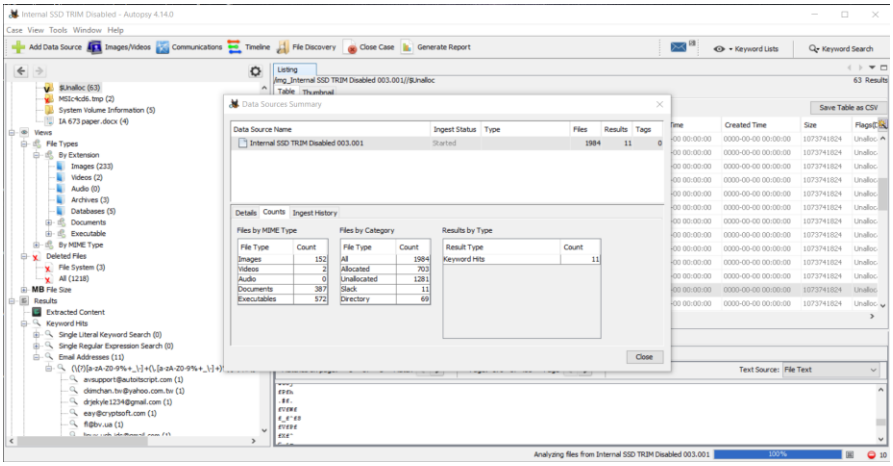

Figure 86. Data Source summary for the Third image

In the keyword search box, we search for indexed words. In the below figure, we searched for "*612 paper 1*, *excel sheet 2*, *puppies*" and got the keyword hits for the Third Image.

We observe that the deleted files are available in log files but are not seen or retrieved in the deleted folder separately, as shown below, except for one file (612 paper).

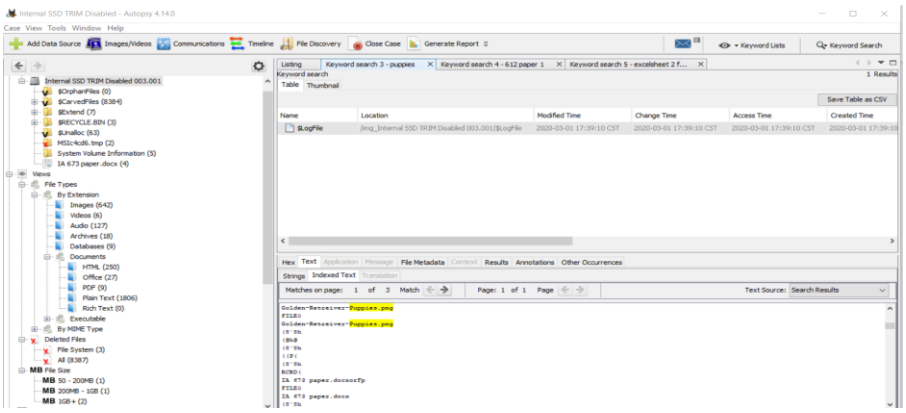

Figure 87. Files found when searched for *"Puppies."*

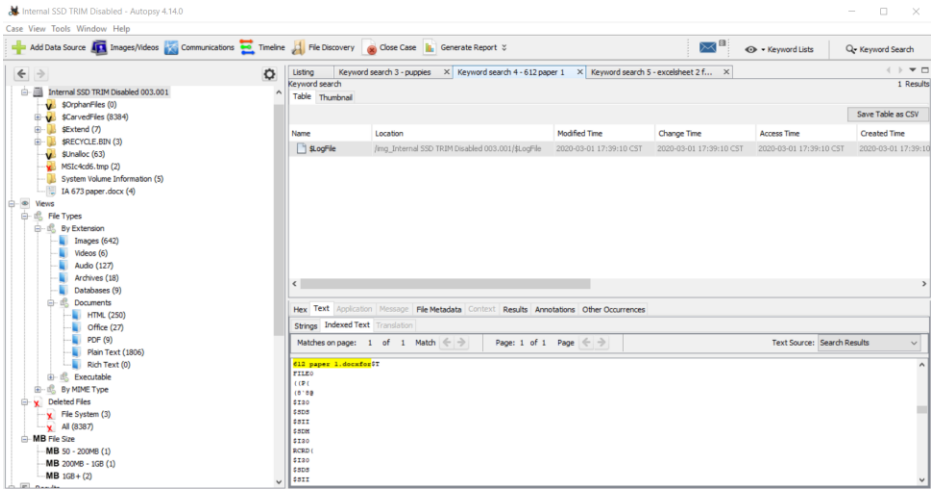

Figure 88. Files found when searched for *"612 paper 1."*

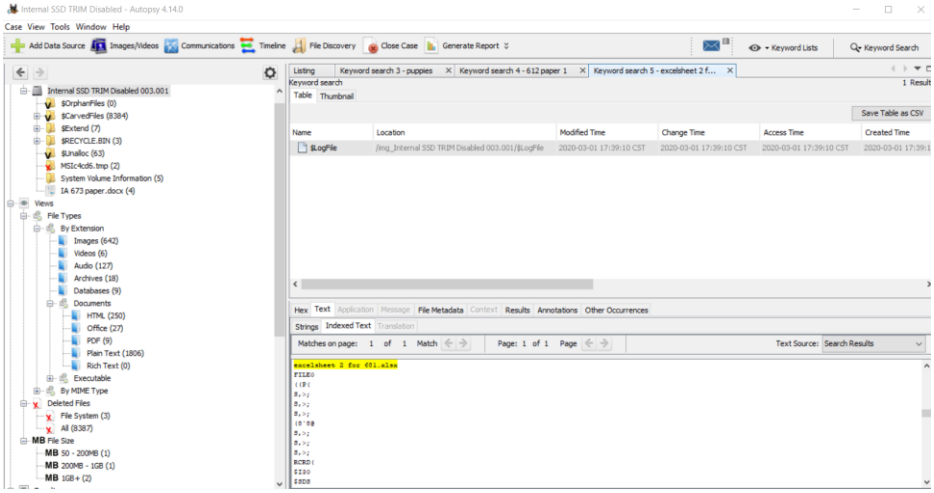

Figure 89. Files found when searched for *"excel sheet 2."*

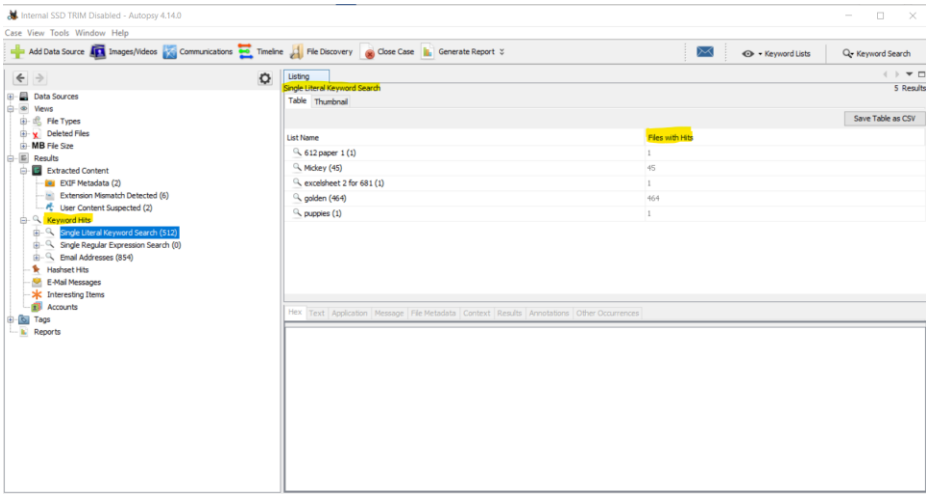

Figure 90. File hits for *"612 paper 1, excel sheet 2, puppies"* for the Third Image

Below is the Autopsy forensic report for the Third Image.

Figure 91. Autopsy forensic report for Internal SSD TRIM disabled

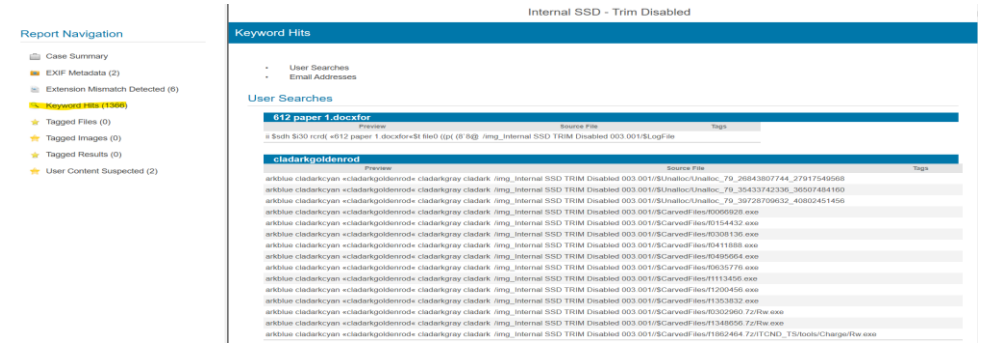

Figure 92. Keyword Hits for Image 3

Image Analysis for Internal SSD when TRIM is Enabled

Now, we analyze the image for Internal SSD when TRIM is enabled. We fill in the case name and give the base directory details where we want the image information to be stored.

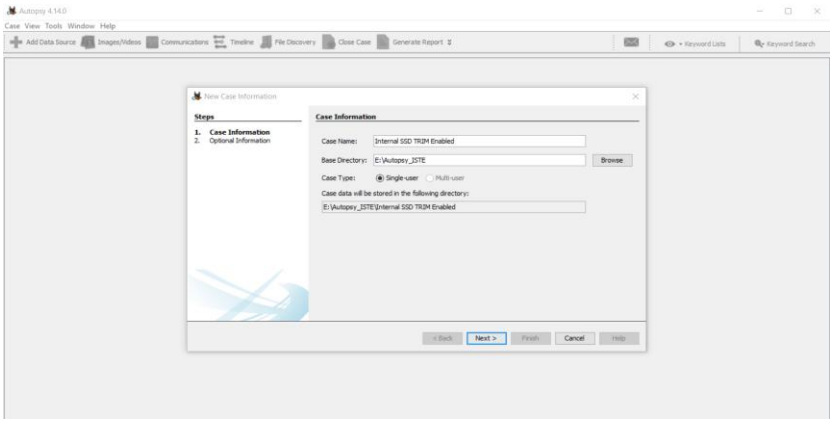

Figure 93. Case information for the Fourth Image

We fill in information such as case number, examiner name, email, phone number, and notes for the Fourth image.

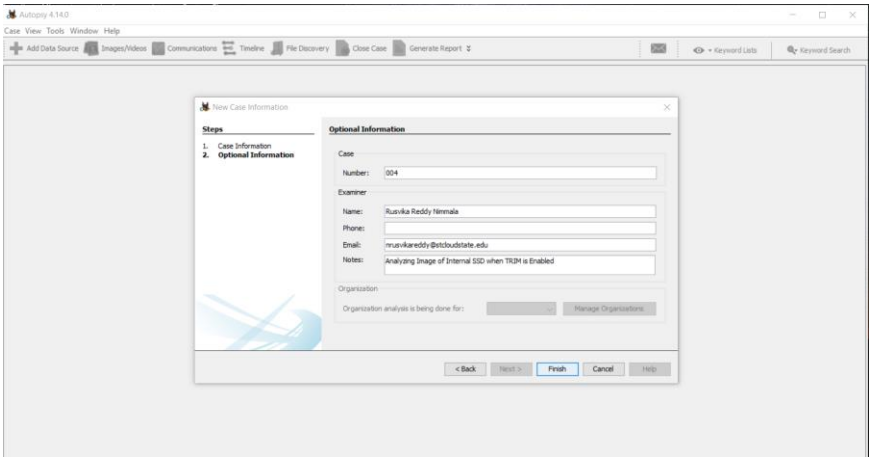

Figure 94. New Case is created for Image 4

Results of Internal SSD when Trim is Enabled

After the analysis is done for the fourth image, we check for the results in a data source summary where we can find files by category, files by mime type.

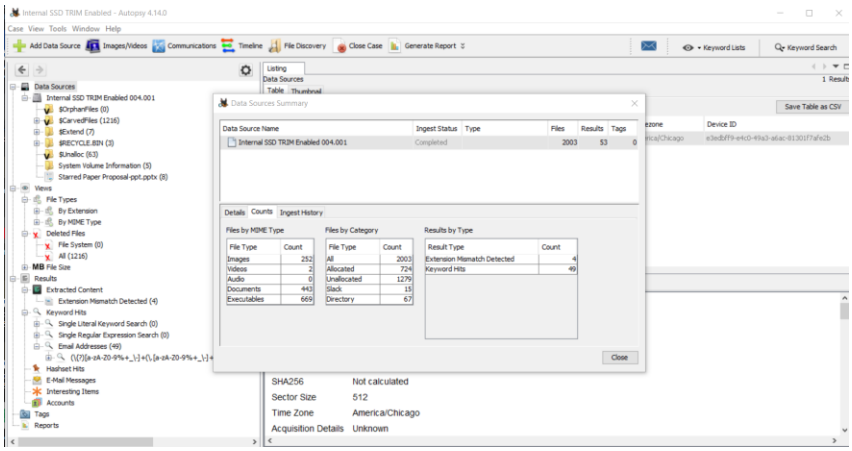

Figure 95. Data Source summary for the Fourth image

In the keyword search box, we search for indexed words. In the below figure, we searched for "*673, mickey and minne, new good one*" and got the keyword hits for the Fourth Image.

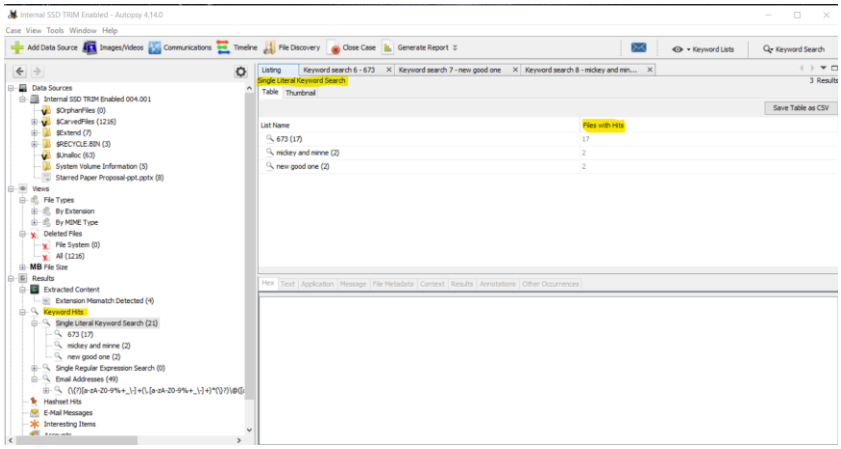

Figure 96. File hits for *673, mickey and minne, a new good one* for the Fourth Image

Here, All the deleted files were only available as a log entry on the image (drive log file).

Below is the Autopsy forensic report for the Fourth Image.

Figure 97. Autopsy forensic report for Internal SSD TRIM Enabled

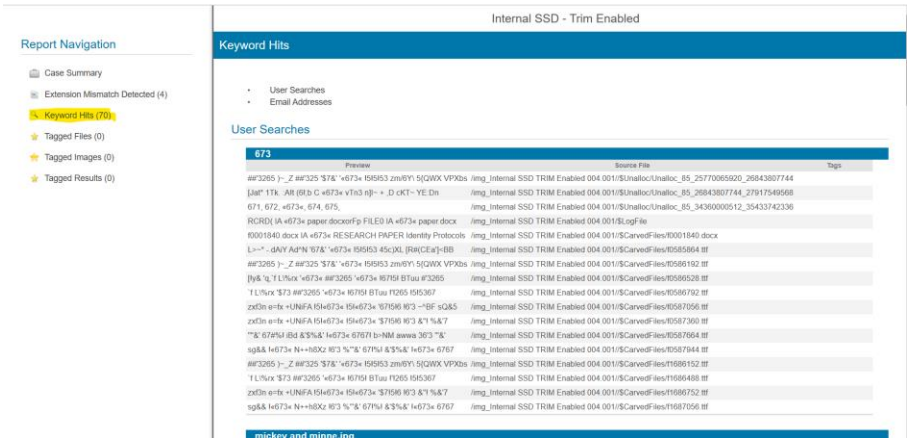

Figure 98. Keyword Hits for Image 4

Summary

In this chapter, we first loaded the data into the drives when TRIM is disabled for both the SSDs. Then we deleted few files while it was on TRIM disabled and added new files. We used FTK Imager to generate an image of these files. Then again, the data was deleted when TRIM is enabled for both the SSDs, and again new files are added, then again, the images are generated for both the drives, and the results are analyzed. The images are mounted onto the Autopsy, and the findings are analyzed with data present on the disks. We compare the results in the next chapter and provide conclusions on the results obtained.

Chapter V: Results, Conclusion and Recommendations

Introduction

In this chapter, we show the results when TRIM was enabled and disabled in both external and internal SSDs. We compare the results which we analyzed through the autopsy tool. We do keyword searches for the files which we deleted. We also analyze the read and write speeds of SSDs for the same.

Results

Table 2

Comparing Internal and External SSDs when they are Disabled

	Internal Disabled			External Disabled		
Keyword Search	No. of Hits	Retrievable files after deletion	Total No. of Files after deleting and adding	No. of Hits	Retrievable files after deletion	Total No. of Files after deleting and adding
612 paper	1	Yes	7	5	Yes	7
Excel sheet 2	1	No	7	4	Yes	7
Puppies	1	No	7	5	No	7

Table 3

Comparing Internal and External SSDs when they are Enabled

	Internal Enabled			External Enabled		
Keyword Search	No. of Hits	Retrievable files after deletion	Total No. of Files after deleting and adding	No. of Hits	Retrievable files after deletion	Total No. of Files after deleting and adding
673 paper	17	No	12	2	No	12
Mickey and Minne	2	No	12	3	No	12
new good one	2	No	12	2	No	12

Table 2 has data for TRIM disabled for Internal and External Solid State Drives. The observation is that only a few of the deleted files were retrievable, whereas the other deleted files were inaccessible. Table 3 has data for TRIM enabled for Internal and External Solid State Drives. The observation recorded here is that the deleted files were not retrievable in all the cases.

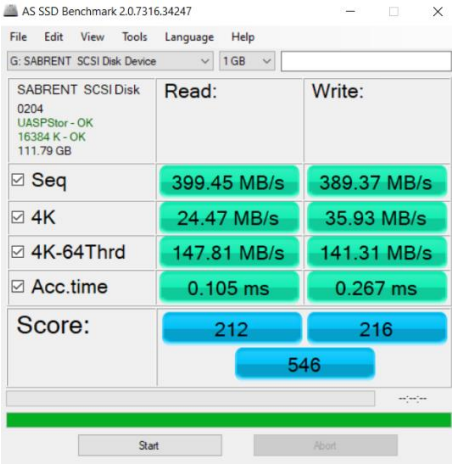

*Figure 99.*External TRIM Disabled

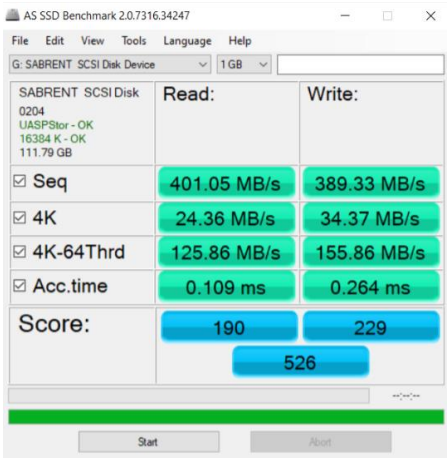

*Figure 100.*External TRIM Enabled

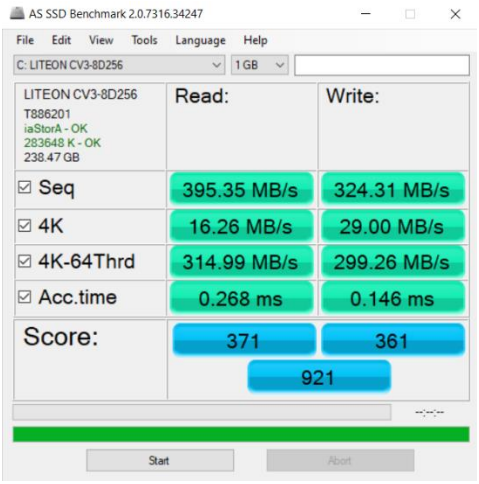

*Figure 101.*Internal TRIM Disabled

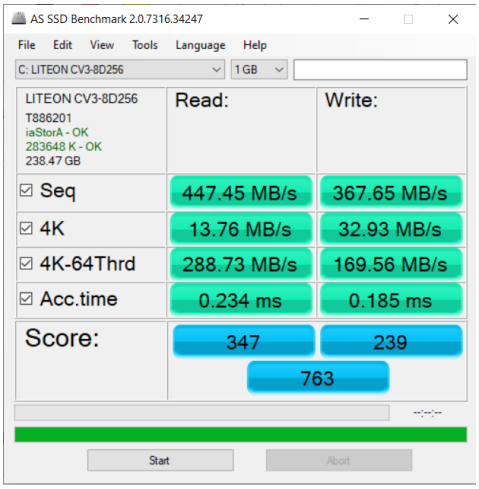

*Figure 102.*Internal TRIM Enabled

From figure 99 and figure 100, we compare the read and write speeds of External SSD. When TRIM is disabled, the read and write speed scores are lower than when the TRIM is enabled.

Similarly, from figure 101 and figure 102, when we compare the read and write speeds of Internal SSD when TRIM is enabled and disabled, the observation is that TRIM disabled has higher read and write speed compared to enabled.

Conclusion

As per the research, we can conclude that while TRIM - ON functionality increases the life span of the SSD and also ensure faster read and write speeds, but it also causes more challenges during forensic investigations. Trim command completely wipes the storage block when a delete command is performed due to which most of the deleted files are inaccessible in forensic investigation tools. As per data in Tables 2 & 3, it is more evident in Internal SSD than in external SSD.

Future Work

There is an exponential increase in use of SSD's in daily life which makes forensic investigation challenging. Future research should be done on TRIM and the architecture of SSD's in such a way that SSD's maintains its unique advantages and also keeps a tab on file history or file activities.

References

A Comprehensive case study on digital forensic. (n.d). Retrieved from https://images.search.yahoo.com/search/images;_ylt=AwrJ6yjFsZpcpXAAWABXNyoA;_ylu=X3oDMTB0N2Noc21lBGNvbG8DYmYxBHBvcwMxBHZ0aWQDBHNlYwNwaXZz?p=digital+forensic+process&fr2=piv-web&fr=mcafee#id=39&iurl=https%3A%2F%2Fmyassignmenthelp.com%2Fmah_cms%2Fuploads%2F

Arora, C. (2019, May 08). *Know What is SSD TRIM Function in Windows and How to Enable and Disable It?* Retrieved from SysToolsgroups: https://www.systoolsgroup.com/how-to/disable-enable-ssd-trim-function-windows/

Belkasoft. (2014, September 23). *Recovering Evidence from SSD Drives in 2014: Understanding TRIM, Garbage Collection and Exclusions*. Retrieved from Forensic Focus: https://articles.forensicfocus.com/2014/09/23/recovering-evidence-from-ssd-drives-in-2014-understanding-trim-garbage-collection-and-exclusions/

Brant, T. (2019, January 29). *SSD Vs HDD: What's the differenece?* Retrieved from pcmag: https://www.pcmag.com/article/297758/ssd-vs-hdd-whats-the-difference

Brinkmann, M. (2010, June 20). *Delete Data On SSD Permanently*. Retrieved from ghacks.net: https://www.ghacks.net/2010/06/20/delete-data-on-ssd-permanently/

Cactus Technologies Wear Leveling-Static, Dynamic and Global. (2019, 03). Retrieved from Cactus-Tech.com: https://www.cactus-tech.com/wp-content/uploads/2019/03/Wear-Leveling-Static-Dynamic-Global.pdf

Casey, E. (2004). Digital Evidence and Computer Crime, Second Edition.

Digital Forensics for Hard drives. (n.d). Retrieved from Gillware: https://www.gillware.com/digital-forensics/hard-drive-forensics-services/?token=77baf832be7f4f96ba932016829a0aea

Dimitrios, D. (2017). *Forensics Research in Solid State Drives.* Athens: University of Piraeus.

Forensic science. (n.d). Retrieved from Wikipedia: https://en.wikipedia.org/wiki/Forensic_science

Geier, F. (2015). The differences between SSD and HDD technology regarding forensic investigations. *Thesis*, 60.

Green, L. (2018, May 17). *Fone Paw*. Retrieved from How to recover data from External Hard Drive: https://www.fonepaw.com/recovery/recover-data-external-drive.html

Gubanov, Y. (2012). *Why SSD Drives Destroy Court Evidence, and What Can Be Done*. Retrieved from Belkasoft Ltd.

HDD Parts. (n.d). Retrieved from https://images.search.yahoo.com/search/images;_ylt=AwrExl8Znp5cE04AZpKJzbkF;_ylu=X3oDMTBsZ29xY3ZzBHNlYwNzZWFyY2gEc2xrA2J1dHRvbg--

;_ylc=X1MDOTYwNjI4NTcEX3IDMgRhY3RuA2NsawRiY2sDMHFwaTdnZGU5ajYwaiUyNmlM0QzJTI2cyUzRGE5BGNzcmNwdmlkAzd6c0Q2REV3TGpJTlprZURYSm1Z

HDD vs. SSD: What does the future for storage hold. (2018, march 6). Retrieved from www.backblaze.com: https://images.search.yahoo.com/search/images;_ylt=AwrJ7J5vRqlcn4cAkglXNyoA;_ylu=X3oDMTE0bWZmNWI0BGNvbG8DYmYxBHBvcwMxBHZ0aWQDQjY4MzNfMQRzZWMDcGl2cw--?p=ssd+vs+hdd&fr2=piv-web&fr=mcafee#id=4&iurl=https%3A%2F%2Fwww.backblaze.com%2Fblog%2Fwp-content%2Fupload

How to Permanently Erase Data Off a Hard Drive. (2019, March 29). Retrieved from wikihow: https://www.wikihow.com/Permanently-Erase-Data-Off-a-Hard-Drive

Hutchinson, L. (2015, April 27). *Modern SSD controllers are super-smart, but using TRIM is still a good idea.* Retrieved from Ars Technica: https://arstechnica.com/gadgets/2015/04/ask-ars-my-ssd-does-garbage-collection-so-i-dont-need-trim-right/

Joshi, B. R., & Hubbard, R. (2016). Forensics Analysis of Solid State Drive(SSD). *Proceedings of 2016 Universal Technology Management Conference (UTMC),Minnesota,United States Of America*, 11.

Patzakis, J. (n.d). New Accounting Reform Laws Push For Technology-Based Document Retention Practices.

Perrin, C. (2011, March 6). *The security limitations of solid-state drives*. Retrieved from Tech Republic: https://www.techrepublic.com/blog/it-security/the-security-limitations-of-solid-state-drives/

Physical damage. (n.d). Retrieved from https://images.search.yahoo.com/search/images?p=physical+destruction+of+hard+disk+images&fr=mcafee&imgurl=http%3A%2F%2Fwww.gizbot.com%2Fimg%2F2016%2F06%2Fharddrivephysicaldamage-24-1466771334.jpg#id=15&iurl=http%3A%2F%2Fallpointsprotects.com%2Fwp-content%

Pros And Cons Computer Forensics. (n.d). Retrieved from PositiveArticles.com: https://positivearticles.com/pros-and-cons-computer-forensics/

Security. (2009). Retrieved from Digital forensic: An introduction. American Board of Information Security.

Slideshare. (n.d). Retrieved from https://images.search.yahoo.com/search/images;_ylt=AwrE1x8sEZxcdpgAJUVXNyoA;_ylu=X3oDMTB0N2Noc21lBGNvbG8DYmYxBHBvcwMxBHZ0aWQDBHNlYwNwaXZz?p=digital+evidence+pictures&fr2=piv-web&fr=mcafee#id=101&iurl=http%3A%2F%2Fimage.slidesharecdn.com%2FIFA8Maart2007Com

Techopedia. (2017, December 12). Retrieved from Solid State Drive (SSD): https://www.techopedia.com/definition/2296/solid-state-drive-ssd

Tokar, L. (2012, April 16). *TRIM in SSDs Explained – An SSD Primer*. Retrieved from The SSD Review: http://www.thessdreview.com/daily-news/latest-buzz/garbage-collection-and-trim-in-ssds-explained-an-ssd-primer/

Trim (computing). (n.d). Retrieved from Wikipedia: https://en.wikipedia.org/wiki/Trim_(computing)#cite_note-Intel_Knowledgebase-1

Varinder. (2016, Nov 1). *Solid State Drive (SSD) The Future of Hard Drives*. Retrieved from SSD: https://images.search.yahoo.com/search/images;_ylt=AwrExdp8haJcMkwAix6JzbkF;_ylu=X3oDMTBsZ29xY3ZzBHNlYwNzZWFyY2gEc2xrA2J1dHRvbg--;_ylc=X1MDOTYwNjI4NTcEX3IDMgRhY3RuA2NsawRiY2sDNWkwOTNzbGRuMTg5bCUyNmIlM0QzJTI2cyUzRHA2BGNzcmNwdmlkAzg0ZS45akV3TGpKWkFTUGxXM0No

Yohannes, F. (2011). *Solid state Drive Digital Forensics construction.* Retrieved from iseek: https://www.politesi.polimi.it/bitstream/10589/37402/3/SSD%20Digital%20forensics%20Construction.pdf

Zhang, S. (2018, March 19). *Data Recovery*. Retrieved from 5 Easy Steps to Recover Hard Drive Data : https://www.datanumen.com/blogs/5-easy-steps-to-recover-hard-drive-data-after-accidental-formatting/

Zubair Shah, A. N. (2015). Forensic Potentials of Solid State Drives. 14.