12-2017

Solid State Drive: New Challenge for Forensic Investigation

Shiva Sai Ram Marupudi
St. Cloud State University, ssmarupudi@stcloudstate.edu

Solid State Drive: New Challenge for Forensic Investigation

by

Shiva Sai Ram Marupudi

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

August, 2017

Starred Paper Committee:
Mark Schmidt, Chairperson
Dien Phan
Balsy Kasi

Abstract

There has been a tremendous increase in the usage of electronic devices day by day. With the increase in usage of electronic devices, technology keeps on emerging. Due to the emergence of new technologies, there has always been a scope for the hackers to cash the loopholes that are available which resulted in a hefty increase in cyber crimes. Consequently, the number of investigations that require digital forensic expertise have been resulting in a huge evidence backlogs that are being encountered by the law enforcement agencies all over the world. It is anticipated that the number of cases that would require digital forensics is likely to be increased in future.

The primary storage technology used for digital information has remained constant over the last two decades in the form of the magnetic disc. For decades, Hard drives have been dominating the market due to their cost and capacity. However, things are being developed and manufactured to be faster and smaller but there are few changes that truly turned to be technological revolutionary. Solid states drive familiarly known as SSD have crept up on us as they arrive under cover of the previously known technology. This paper demonstrated that the assumptions about the behavior of a storage media are no longer valid, how modern storage devices will operate under their own volition without any computer instructions. These operations are highly destructive of traditionally recoverable data. This would contaminate evidence, can make validation of digital evidence reports difficult, it can complicate the process of live and dead analysis recovery and can also complicate and frustrate the post recovery forensic analysis. This paper compared the key evidence that were identified in an HDD and SSD and discussed the key features that make SSD self-Destructive and cause difficulties for Forensic Investigations.

Table of Contents

Chapter Page

Chapter Page

List of Tables

Table Page

List of Figures

Figure Page

Figure Page

Figure Page

Figure Page

Figure Page

Chapter I: Introduction

Introduction

Digital forensics (n.d.) is the collection and analysis of data from computers and digital devices such as mobiles for obtaining an evidence . Digital forensics has played a very crucial role over the past three decades in criminal, civil or corporate investigations. There are few areas of dispute or crime in which computer forensics cannot be applied. The earliest and heaviest users of digital forensics have been law enforcement agencies and they have been consequently at the forefront for the development of the field.

Computers are often prone to hacking or denial of service attacks and they hold evidence in the form of documents, internet history, emails and other files which are relevant to crimes such as fraud, drug trafficking, murder, and kidnap. Computer constitutes a ‘scene of crime.’ Not only the content of documents, emails and other files which create interest to the investigators but also metadata that is associated with the files. A forensic examination would report when a document is being created, when was it first found in the system, when it was last edited, when was it last modified, last saved, or printed and the user who carried all these operations (Justice, 2007).

Many commercial organizations have been using forensics for their benefit in a variety of cases such as bankruptcy investigations, employment disputes, industrial espionage, regulatory compliance, fraud investigations, forgeries, intellectual property theft, inappropriate email, and internet use in the workplace.

As per some of the estimates, it states that almost 95% of the criminal cases would leave evidence that could be captured and analyzed through a common computer forensic procedure.

Many of the criminals are getting smarter these days, data hiding techniques such as steganography and encryption can put evidence of criminal activity where in traditional search methods cannot be able to find them. Encryption is scrambling data such as an email message so that it cannot be read if it is intercepted in transit. Steganography is hiding the message in a larger file typically like in a photographic image or in a sound file.

Computer forensics is not just about the detective work,i.e.,searching for and attempting for discovering information. It is also concerned with handling the sensitive data responsibly and confidentially. It about taking certain precautions to ensure the integrity of data, taking precaution to not nullify findings by corrupting the data and staying within law and rules of evidence (Service, 2009).

Following are the steps that are common in all forensic investigations (Security, 2009):

(a) Collection, (b) Examination, (c) Analysis, and (d) Reporting.

Figure 1. The Forensic Process (Security, 2009)

- **Collection.** Identify, 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 analysis being 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.

The most frequently investigated are Identifying the theft, Fraud, and embezzlement, Software privacy and hacking, Blackmail and extortion, Child Pornography and Exploitation, Terrorism and national security, Prostitution, infidelity, domestic violence, Theft of intellectual property and trade secrets (Ashcroft, 2001).

The evidence that can be recovered in Network Intrusion and Hacking investigations include Network usernames, Internet protocol addresses, executable files, security logs, configuration files, text files and other documents containing sensitive information such as passwords. Evidence can be recovered in Identifying Theft investigations include Identification of templates, electronic images and signatures, credit card numbers, online trading information and credit card reader/writer/scanner. In Harassment and stalking investigations, we can recover victim background information, maps to victim locations, photos, diaries, internet activity logs, emails, notes, and letters (Solomon, 2005).

Problem Statement

Day-by-day technology is developing, even the hackers are getting updated with the new technology and are becoming more powerful. The crime rate has been increasing day by day. There are many cases which can be solved using digital forensics. However, these days due to the advanced technology utilized by the Solid-state drives is posing a risk of finding the key

evidence when compared to that of magnetic hard disk drives. Digital forensics has found some traditional mechanism for cracking the evidence easily for hard drives as they are working on the same from decades. However, these mechanisms cannot be applied to solid state drives due to advanced features. This paper research problem is to investigate the key factors which are causing risk for the forensic investigators for finding evidence in solid state drives, analyze the results obtained from both hard drives and solid-state drives.

Nature and Significance of the Problem

Digital forensics plays a very crucial role in solving some complex cases. Forensic investigators have followed some traditional mechanisms for solving these cases on hard drives. As technology keeps on changing day by day, we are currently using solid state drives which came in as a competitor for hard disk drives. However, the mechanisms that were successful for cracking evidence in hard drives were not successful in the case of solid state drives (Kipp, 2015). As per the recent analysis, it was found that 40 out of 100 people are opting for solid state drive instead of a hard drive. If this continues and when we reach a stage wherein there are only solid-state drives and no hard drives will digital forensic be able to solve these cases? What exactly is the reason behind the evidence destruction in solid state drive? This paper provides the key features of solid state drive which trouble forensic investigators and compares the results obtained from a hard disk and a solid-state drive.

Objective of the Study

The main objective of the study is to find out why the forensic investigators are facing troubles finding evidence in SSD's when compared to that of HDD's. This study will also compare the results obtained from Hard disk drives and solid-state drives by using a forensic tool.

Study Questions

The study questions revolve around the challenges being faced by digital forensics due to solid state drives, why solid-state drives destroy the court evidence and what can be done about it and what is the importance of TRIM on an SSD.

Limitations of Study

This study does not attempt to change the existing methods for extracting evidences, but only suggests the different challenges being faced by the forensic investigators using the traditional methods for extracting key evidences, explains the different evidence destruction mechanisms available in an SSD which help destructing the evidences.

Definition of Terms

Digital forensics. Digital forensics (sometimes known as digital forensic science) is a branch of forensic science encompassing the recovery and investigation of material found in digital devices, often in relation to computer crime. The term digital forensics was originally used as a synonym for computer forensics but has expanded to cover investigation of all devices capable of storing digital data. With roots in the personal computing revolution of the late 1970s and early 1980s, the discipline evolved in a haphazard manner during the 1990s, and it was not until the early 21st Century that national policies emerged (wikipedia, 2005).

*Hard disk drive***.** A hard disk drive (HDD), hard disk, hard drive or fixed disk is a data storage device that uses magnetic storage to store and retrieve digital information using one or more rigid rapidly rotating disks (platters) coated with magnetic material. The platters are paired with magnetic heads, usually arranged on a moving actuator arm, which read and write data to the platter surfaces. Data is accessed in a random-access manner, meaning that individual blocks of data can be stored or retrieved in any order and not only sequentially. HDDs

are a type of non-volatile storage, retaining stored data even when powered off (Hard disk drive, n.d.).

Solid state drive. A solid-state drive (SSD, also known as a solid-state disk) is a solid-state storage device that uses integrated circuit assemblies as memory to store data persistently. SSD technology primarily uses electronic interfaces compatible with traditional block input/output (I/O) hard disk drives (HDDs), which permit simple replacements in common applications. New I/O interfaces like SATA Express and M.2 have been designed to address specific requirements of the SSD technology (Solid state drive, n.d.).

Summary

In this section, we had an introduction of what is digital forensics. The steps that are being followed in a forensic investigation. As crimes have been increasing daily the need for digital forensics has been increasing day by day for solving some of the most crucial cases. However forensic investigators are facing some tough time with the advanced storage device named solid-state drives. What makes solid-state drives more difficult to crack for investigators who have been successful over decades over hard disk drives? What are the special features this drive has? How is it able to destroy the evidence? Comparing of the evidence obtained from both these drives is a crucial part of this research. In next chapter, we are going the discuss in detail about the problem and the mechanism of operation of both the HDD and SSD.

Chapter II: Background and Review of Literature

Introduction

To understand the problems faced by forensic investigators in cracking evidence from a solid-state drive when compared to that of a hard disk drive, we first need to understand the functioning of both these drives. Although both are meant to store information, the way information is being stored, what happens when data is being modified and when data is deleted is the key to understanding the challenges in retrieving information. In this chapter, we will be discussing the functioning of hard disk drives and solid-state drives in details, in detail functioning of each part, the concept used for the storage of information.

Background Related to Problem

Hard disk drives and Solid-state drives are used for storing information in a personal computer, Laptop, tablets. Although both the drives are meant to look similar and have the same purpose,i.e.,storing information the mechanism behind the working of these drives is completely different. Due to the change in the mechanism and some special features in a Solid-State Drive, the forensic investigators are not able to follow the same traditional method that was successful over decades for retrieving evidence in a hard disk drive over in solid-state drive. So, let us discuss in detail the mechanism involved in both drives.

Literature Related to the Problem

Hard Drives

Like many inventions that took place in 20th Century computing, hard drives are being invented at IBM as a way that could help computers with a rapidly accessible Random-Access Memory. Many other computer memory devices such as punched cards and reels of magnetic tapes had issues with accessing the data. Data could be accessed serially only, i.e., from

beginning to end. So. If I was trying to retrieve some information which is in the middle of the tape, you need to scan or read entire thing slowly to find out what you want. All the issues were being fixed in Hard drives which have the capability to move from one part of the disk to other very quickly and access the information easily. IBM's Reynold B. Johnson developed the first hard drive and announced it on September 4, 1956 as the IBM 350 Disk Storage Unit (Bodo, 1996).

Hard drives are the most widely used storage devices from over decades. A hard drive is an incredibly efficient computer memory device that uses the concept of a simple magnetism to store a very vast amount of information. They have been invented 50 years ago, and have been used in the personal computer from the mid-1980s. Thinking and calculating is being done by the microprocessor on your computer, but it is the hard drive that gives a computer its prodigious memory and helps to store digital photos, text documents, music files and much more (Mamun, Guo, & Bi, 2007). But how does it work?

Storing Information using Magnetism

It is very complex to understand the science of magnetism. But by understanding the technology with the help of a magnet and nails,i.e.,the science in action it is very simple. A simple iron nail is unmagnetized, but if you rub a magnet back and front over them then they tend to use the magnetic power and stick to one another. Magnetism has some practical, simple uses. Considering the example of junkyards which use electromagnets for picking and moving around piles of a metal scrap (Daniel, 2011).

Magnetism has another important use. Suppose you are looking to leave a message for a friend, all you have is a magnet and an unmagnetized iron nail. The message which you need to convey is a simple one,i.e.,either if you are going to meet your friend in the evening or if you

cannot make it. So, you choose to leave a nail in your friend's mailbox as a means of communication on your decision. The concept behind the nail is simple, if the nail is magnetized then you will be meeting him in the evening and the vice versa if the nail is unmagnetized. Once your friend reaches home and checks his mailbox he finds a nail, he then collects it and uses a paper clip to verify whether it is magnetized or unmagnetized. By using the result, he concludes whether you will be meeting him or not. Here the iron nail is storing information of your meeting. So, magnetism can be used to store information.

Relating the concept which is illustrated above let us see how it works in computers. Suppose you have a computer that has a hard drive of 20-gigabyte capacity, it is like a box which contains 160,000 microscopically small iron nails, each nail would store a tiny piece of information known as a bit. The bit is a binary digit which can be either a number 1 or number 0. In computers, information is being stored in the pattern of binary digits. For example, a computer stores a capital letter A as a decimal number 65 also represented as 1000001. So, for storing the information in a big box of nails,i.e.,your computer you would magnetize the first nail for storing 1 and demagnetize the next five digits for storing 0 and magnetize the last digit to store 1.

Hard Drive Functioning

It is very difficult to hold 160,000 nails in a big box and use it as a hard drive in your computer. So, the hard drives that we use do not really contain any nails. The hard drive contains a large shiny circular plate of magnetic material known as a platter which is divided into billions of tiny areas. Each of these areas can be independently magnetized to store a 1 or demagnetized to store a 0. The concept of magnetism is used in a computer to store information even there is no power supply. This is the same concept of an iron nail which stays magnetized until we demagnetize it.

Figure 2. Hard Drive Components (Woodford, 2015)

A hard drive has only a few basic parts. There are one or more silver platters where the information is being stored magnetically, an arm mechanism that helps move a tiny magnet known as a read-write head back and front over the platters for recording and storing the information. There is an electronic circuit that controls everything and would act as a link between your hard drive and your computer (Mamun et al., 2007).

1. The actuator moves the read-write arm. In earlier hard drives, stepper motors were used for moving the read-write arm. In the latest hard drives, voice coils are being used. As the name resembles these are simple electromagnets working like the moving coils that make sounds in loudspeakers. They are less sensitive to problems like temperature variations and position the read-write arm more reliably, precisely, and quickly when compared to stepper motors.
2. Read-write arm swings the read-write head both back and forth across the platter.
3. Central spindle helps the platter to rotate at a high speed.
4. Information is being stored in the Binary form in a Magnetic platter.
5. The hard drive is being linked to the circuit board in a personal computer by the help of plug connections.

6. A tiny magnet at the end of the read-write arm is the read-write head.
7. The flow of data to and from the platter is controlled by the circuit board.
8. The flexible connector is used to carry the data from the circuit board to read-write header and platter.
9. Spindle helps the read-write arm to swing across the platter.

The most important part of hard drives is platters. They are made up of a hard material such as glass and aluminum, coated with a thin layer of metal which can be demagnetized and magnetized. A hard drive of the small size typically has a single platter, each side has a magnetic coating. Bigger hard drives have a series of platters that are being stacked up on a central spindle with small gaps between them. Platters typically rotate at 10000 revolutions per minute so that the read-write headers can access any part of them. Each platter has two read-write heads, one which could read the top surface and other which could read the bottom surface. Read-write are being mounted on an electronically controlled arm which moves from center of the drive to the outer edge and back again. Reducing the wear and tear the read-write head does not touch the magnetic platter, there is a layer of air or fluid in between them,i.e.,in between the head and the magnetic platter surface (Mueller, 2015).

Reading and Writing Data

Storing the information is not a big task, but to find the information whenever it is needed is a tough task to do. Suppose you are storing a nail in a pile of 1.6 million identical nails and at a later point of time if you need to get hold of this nail and if there is no methodical way for doing this then it would take hours or days for doing so. Now relating the same to the computer, if it did not use a very methodical way, we can imagine the pain it gets through for finding that simple information.

When information is being stored on a hard drive by the computer, it does not just throw the magnetized nails into a box with all jumbled together. On each platter, data is being stored in very orderly manner. Bits of data are being arranged in concentric circular paths called tracks. Tracks are being broken into smaller areas known as sectors. Part of the hard drive stores sectors that are already been used up and others which are still free. This map is known as File Allocation Table in windows. When the computer needs to store some information, it looks at the file allocation table or the map to find some free sectors for storing the information. Once it could locate some free sectors then it instructs the read-write head to move across the platter exactly to the right location and store the information there. For reading the information the same process is being followed in a reverse manner (Bajorek, 2014).

Figure 3. Actuator Arm. Left: The Actuator arm will swing the head back and forth to ensure it is in the exact position on the drive. Right: The extreme tiny end of the hard drive that writes to and reads from the platter (Woodford, 2015)

Hard Drive is a remarkable piece of engineering with so much information being stored in a tiny space. There are certain drawbacks too, one of that is hard drives can go wrong if they get dirt or dust inside them. The read-write head can be bounced up and down and may crash into the platter resulting n damaging the magnetic material due to a tiny piece of dust. This is also known as a disk crash or a head crash which could result in loss of information on a hard drive.

Solid State Drives

A solid state drive (SSD) is a solid-state storage device that uses an integrated circuit assembly as a memory to store data persistently. SSD's do not have any moving mechanical components. Solid state drive uses a semiconductor chip, not magnetic media for storing data. Over the past few decades, there has been a considerable amount of work being done in the field of computers hardware. Even though the computer technology has been constantly improving and evolving we rarely experience that feeling where we sit back and say, "wow that's amazing." It is very rare to find a computer upgrade that would single-handedly transform our desktop experience. We might be replacing a monitor with the latest led technology, upgrade our video card for the best gaming experience, or install an additional RAM for faster processing. However, the experience would feel the same at the end. But when there is a switch from hard drive to solid state drive suddenly everything is fast (Aaronson, 2008).

For understanding the SSD technology, we would need to understand the basic overview of computer architecture. To make it simple, the computer's memory architecture is being divided into three sections namely cache, memory, and hard disk. Each section has a critical function that determines the way they operate.

Cache is the innermost memory unit. Cache is used as a sort of playground for doing all calculation and procedures as the computer operates. The data access is instantaneous, electrical pathways to the cache are the shortest because the cache is mandatory. Memory is the middle ground for computer known as RAM, Random Access Memory. RAM is the place where information is being stored related to processes running on your machine and active programs. Access to the memory is slow when compared to that of cache. A hard disk is a place where everything is being stored for performance. Hard disk stores all our configuration files,

programs, music files, documents, and more. When a file is needed to be accessed or when we need to run a program it needs to be loaded from the hard disk and then into the memory (Evans, 2012).

There is a vast difference in speeds. Cache and memory operate at a speed of nanoseconds, hard disk operates at a speed of milliseconds. The reason behind the change in speeds is to do the spinning of the hard drive, it needs to spin to the right location for retrieving information. So, it is clear that before the computer can do anything it needs to wait for the response from the hard disk. The hard disk is the key bottleneck, no matter how fast everything else works, the faster the hard disk works the faster we can operate. This gave an advantage for the SSD to step in. The bottleneck would be cut down by a factor of 10, single handling by cutting a massive chunk of wait time when using a computer.

SSD: How they Operate?

Solid state drives use memory known as “flash memory” that is similar to a RAM. However, RAM clears whenever the computer is power down but SSD memory would remain the same even there is a power loss. SSD’s use a grid of electrical cells for sending and receiving data. Grids are being separated in the section known as pages, pages are the place where data is being stored. These pages clumped together and form blocks. SSD can write to empty pages in a block, in Hard disk data can be written to any location on the magnetic plate at any time,i.e.,data can be overwritten easily. SSD’s cannot overwrite the data, SSD should first find an empty page in the block and write data to that empty page. When enough pages in the block are being marked as unused the SSD will take the content of the block, commit that to the memory, and would erase the whole block. Once it is done, it would take the committed image and will reprint it on that block without unused pages (Goble, 2012).

How SSD Work

To understand the functioning of an SSD, we first need to know the two most important parts: The controller and NAND flash memory. These components along with few others are being placed on a PCB known as printed circuit board which is being housed in a casing known as SSD.

Controller. Controller is an embedded processor that bridges the flash memory components to host, i.e., computer. The controller executes the codes that are provided by the SSD's firmware, i.e., the mini operating system to fulfill data requests received from the host. The controller would decide how SSD would perform and the features it offers. The popular functions and features decided by the controller include reading, writing, error checking, erasing, garbage collection, encryption, wear-levelling, overprovisioning, and RAISE (Seagate, 2012).

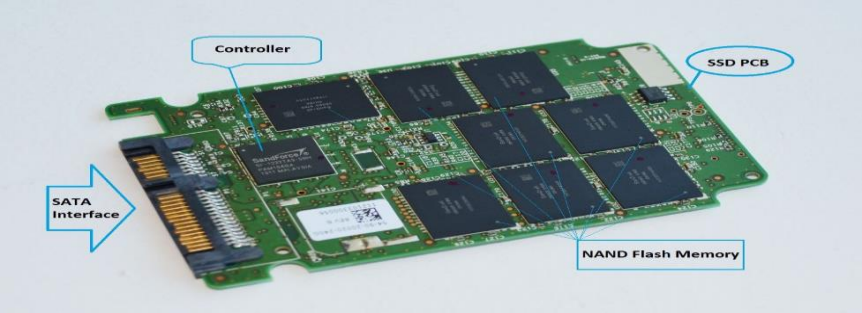

Figure 4. Solid State Drive (Ngo, 2013)

NAND Flash Memory

Modern solid-state drives use NAND flash memory which is an integrated circuit designed for storing information. Enterprise solid state drives use a single-layer cell NAND, i.e., SLC NAND, whereas consumer grade SSD's use a multilayer cell NAND. The former is fast and would last longer than the latter; however, it is more expensive. As these are not magnetic platters, writing to an SSD occurs when the controller programs the memory cells for storing the

information. The memory shell would store voltage and would be either on 1 or 0 state, which allows them to store data in binary form. Come to reality writing data to an SSD is a complicated process. However, reading data is relatively simple because the controller does not have a lot to work to do (Masuoka, 1987).

These NAND flash memory cells come with some interesting attributes. Firstly, they can be programmed for a limit amount of time before they become unreliable. This is known as a program-erase (P/E) cycle or write endurance. For reducing this effect, the controller uses a technique named wear-levelling which makes sure that the drive's memory chips are being used effectively cell by cell before the first cell could be written on again. Secondly, unlike the Hard drives, NAND flash memory cannot overwrite the existing data. Old data must be erased before new data can be written to the same location. The inefficiency in erasing data is the third attribute of flash memory. In an SSD the memory cells are being grouped together into a page,i.e.,typically 4kb each and the pages are being grouped together into blocks which are typically 512kb each or 128 pages. Data can be written page by page; however, it can only be erased block by block (Hutchinson, 2012).

When we try to delete some data or even empty the recycle bin in an SSD, there would be no erasing taking place. The operating system such as Windows which uses a TRIM command would just mark the data that you wanted to erase as invalid or stale page by page. However, the actual erasing is being done only when the user writes new data to the drive. So, until and unless you are using the SSD drive for the first time, there would be no writing to that drive that happens without erasing taking place first. This would result in a controller having to do something known as garbage collection while writing data to SSD. Wear leveling and garbage

collection would cause the data to be re-written on SSD from one place to another with a phenomenon called as write amplification.

Drawbacks of SSD

The main problem behind SSDs is inherent in the flash memory, i.e., it could sustain only a finite number of writes before it dies. There is a lot of science which goes in to explain the phenomenon behind this, but it suffices to say that, when an SSD has used the electrical charges within, the cells must be periodically reset. Unfortunately, the electrical resistance increases slightly during every reset which increases the voltage necessary to write in a cell. The voltage becomes so high that the cell becomes useless. Thus, there are a finite number of writes (Ngo, 2012).

Literature Related to Methodology

The functioning of hard disk drive and solid-state drive is discussed in the above section. Now we have a clear picture of what happens when we write data to an HDD or SSD. When data is deleted or modified, there are some predefined mechanisms that undergo in both HDD and SSD, these help the forensic investigators in retrieving key evidence. In this paper, we are going to compare the results obtained from both hard disk drive and a solid-state drive when data is modified, deleted, or updated, and analyze these results. The mechanisms are different in both hard disk drive and a solid-state drive. Following is a general comparison of a solid-state drive and a hard disk drive.

SSD vs. HDD

Both Hard drives and SSDs do the same job of booting our system and storing our applications and our personal files. But each type of storage has its own unique feature set. Let us now discuss how they differ with one another.

Price. SSDs are expensive when compared with that of Hard drives in terms of dollar rate per Gigabyte. A 1 Tb internal hard disk is available for around $40-50; however, an SSD with the storage capacity would cost you around $200.. Translating it to per gigabyte, it would cost 4 to 5 cents per gigabyte for a Hard drive and 19 to 20 cents per gigabyte for a solid-state drive. Since the hard drives use the older and most established technology they will remain inexpensive for near future. Extra hundreds would push our system price over budget in case of SSD (Domingo, 2017).

Maximum and common capacity. The maximum capacity at present that is provided by an SSD is 4Tb, these are rare and costly to find. In the case of hard-drives, we generally find 500 GB to 1 TB as the primary drives for systems. In 2017, the base hard drive is 500gb, pricing concerns push it down to 128gb for SSDs. Multimedia users would require even more, i.e., 1TB to 4TB drives common in high-end systems. As the storage capacity increases, more stuff could be kept on your PC. Cloud-based technology is good for housing files that we plan to share among our phone, PC, and tablet, but the local storage is inexpensive and we should buy it once.

Figure 5. HDD vs. SSD Comparison. Similar outside appearance, however, no common internally of an SSD and HDD (Ngo, 2013)

Speed. This feature makes SSD shine over HDD. An SSD based system would generally boot within a minute and mostly in just seconds. A hard drive would require time to speed up to operating specifications and it would continue to be slower than an SSD during the normal use.

A personal computer or a MAC with SSD would boot faster, launch, and run apps faster and transfer the files faster. Whether we are using our computer for fun, business or school works this extra speed would be the difference between finishing on time and lagging (Hesse, 2017).

Fragmentation. Due to larger recording surfaces, hard drives will work best for larger files that are being laid in continuous blocks. The drive head can start and end its read in one continuous motion. Large files become scattered around the disk platter causing the drive to suffer from fragmentation when hard drives start to fill up. The read-write algorithms have improved to point out that the effect is minimized, however, hard drives can still become fragmented. SSDs do not get fragmented; however, the lack of physical head means that data can be stored anywhere. Thus, the SSDs are faster.

Durability. SSD does not have any moving parts in it, so it is likely that your data is safe in event of dropping your laptop bag or any damage due to mishandling. Most hard drives would park their read-write heads when the system is turned off, but the head would be flying over the magnetic plate within nanometers distance during operation. Even though the head is being parked when turned off, the brakes have certain limits. So, it is recommended for SSD for rough operation (Devine, 2016).

Availability. Hard drives are plentiful in the budget and older systems. SSDs are becoming prevalent in recently released laptops. Product lists from Toshiba, Hitachi, Seagate, and Samsung are still skewed in favor of hard drives rather than SSDs. PCs and MAC desktops will have internal hard drives at least for the next couple of years. SSD model lines are growing day by day in number. The witness is the number of thin laptops with 256 to 512 GB SSD installed in replacement of hard drives.

Form factors. Since hard drives consist of spinning platters, there is a limit for how small they could be manufactured. There was an initiative made for the development of a 1.8-inch spinning hard drive but it was stalled at about 320GB, as phablet and smartphone manufacturers have settled on flash memory as primary storage. SSD does not have any such limitation, as time goes on they can shrink further. SSDs are available in 2.5-inch laptop drive sized boxes, but it is just for convenience. As laptops continue to become slimmer and as tablets take over as the primary platforms for web surfing, then we would see the adoption of SSDs skyrocket (Brendan, 2017).

Noise. Even quietest hard drive would make some noise during the drive spinning or read arm moving back and forth, particularly when it is in a system that is been banged about or if it is improperly installed in an all metal system. Faster hard drives will make more noise when compared to that of slower. SSDs do not make any noise as they are non-mechanical.

As far as longevity, it is true that SSDs would wear out over time. TRIM command technology dynamically optimizes the read-write cycles, you are more likely to discard the system for obsolescence after six years or so before you get started with read write errors with an SSD. There are several tools that monitor the S.M.A.R.T status of your SSD or Hard drive and would let us know if we are approaching the drives end of life.

Following is a tabular comparison of hard drives and solid-state drives:

Table 1. *Comparison of HDD and SSD* (Baxter, 2015)

Attribute	Solid State Drive	Hard Disk Drive
Battery Life/ Power Draw	Less power draw, averages 2-3 watts which result in 30 plus minutes' battery boost	More power draw, averages up to 6-7 watts and therefore would use more battery
Capacity	Not larger than 1TB for notebook size drives and 4TB maximum for desktops	Around 500 GB and 2TB maximum for notebook size drives and 10TB for desktops
Noise	No moving materials and so no such sounds	Audible clicks and spinning can be heard
Cost	Costly, around $ 0.23 per gigabyte based on the buying a 1TB drive	Cheap, around $ 0.03 per gigabyte, very cheap buying a 4TB model
Operating system Boot time	Around 10-13 seconds of average boot time	Around 30-40 seconds of average boot time
Heat Produced	Lower power drawn and no moving parts. So little heat is produced.	HDD does not produce much heat. It has a measurable amount more heat than SSD due to moving parts and higher power draw
Vibration	As there are no spinning or moving parts there are no signs of vibration	The spinning of the platters can sometimes result in vibration
Failure Rate	Mean time between failure rate of 2.0 million hours	Mean time between failure rate of 1.5 million hours
Encryption	Full Disk Encryption (FDE) is supported on some models	Full Disk Encryption (FDE) is supported on some models
File Opening Speed	Up to 30% faster than HDD	Slower than SSD
File Copy/ Write Speed	Generally, above 200 MB/s and up to 550 MB/s for cutting edge drives	The range can be anywhere from 50-120MB/s
Magnetism Affected?	An SSD is safe from any effects of magnetism	Magnets can erase data

Summary

In this chapter, we discussed the mechanism behind the functioning of both solid-state drives and hard disk drives. We discussed on how the drives store information, how they are different from each other, the main components of a hard disk drive such as magnetic platter which is used for storing information, actuator, spindle, read-write arm. Similarly, the main components of a solid-state drive such as the controller and NAND flash memory and functioning of them. These key concepts will help us understand the key features in a solid-state drive which possess a risk to the forensic investigators in the next chapter.

Chapter III: Methodology

Introduction

In this chapter, we will be discussing on the methodology that is being used in this research. We will also be discussing the key features such as garbage collection, wear leveling, TRIM, over provisioning, write amplification, raise and IOPS. We will be discussing on the data collection techniques, tools and techniques being used and hardware and software requirements that are necessary for the experiment.

Design of the Study

This study involves comparison of evidence obtained from a solid-state drive and a hard disk drive. A quantitative research approach is best suitable for my research, as it helps in comparison of the data statistically. In this study, we will initially send a file which involves some key evidence required for solving a case, and some random data such as images, documents. This file is being copied to both a hard disk drive and a solid-state drive. Both the files are deleted and a random data is being copied on both the drives. Random data is being added along with the evidence by different combinations. The drives are formatted after each combination and refilled with new data. A forensic tool named FTK imager is used for creating an image of the disk and FTK Toolkit for solving this case by finding the key evidence. The results obtained from HDD are set as a hypothesis for the study. The same process is followed in a solid-state drive. The results obtained in these two cases are compared statistically and it will help us understand the challenges that are being faced by forensic investigators for cracking the evidence in solid state drives.

Data Collection Model

The process involves three different laptops, one is a Dell Inspiron 13- i7359 with an SSD SanDisk z400s 2.5 7mm 256gb, Intel® Core™ i7 – 6500 CPU @ 2.50GHZ, second laptop Lenovo Flex 4 with an SSD 256gb, Intel® Core™ i7 – 6500 CPU @ 2.50GHZ and an investigator laptop Dell Inspiron 13- 7348 with an HDD ST500LM000-1EJ162, Intel® Core™ i7 – 5500 CPU @ 2.40GHZ. A random data involving multiple word documents, images, bulk emails, bulk files, media is created. Both laptops are running Windows 10 operating system. A brand new SSD of 512 GB and an HDD of 1TB is used for this experiment.

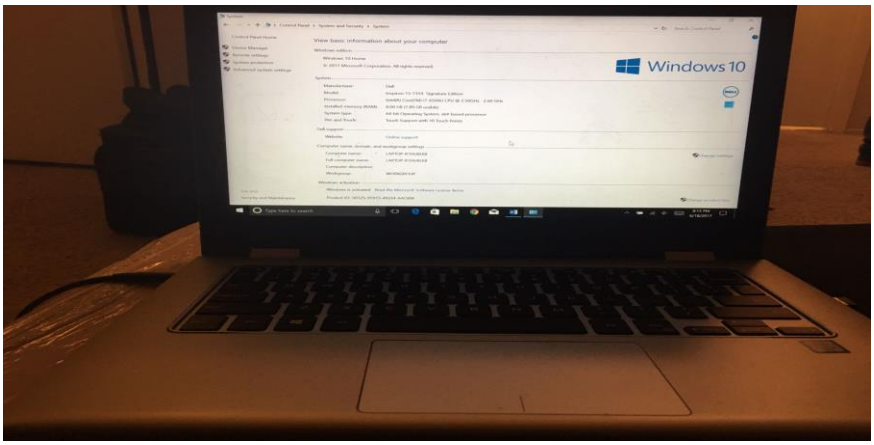

Figure 6. Dell Inspiron 13 - i7359

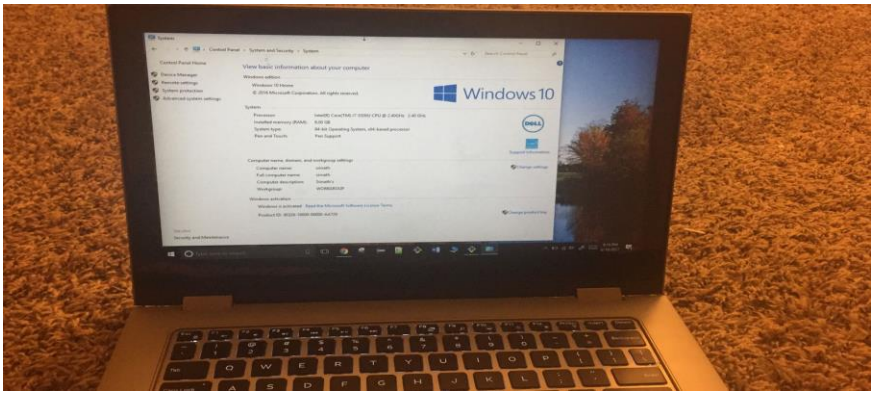

Figure 7. Dell Inspiron 13 -7348

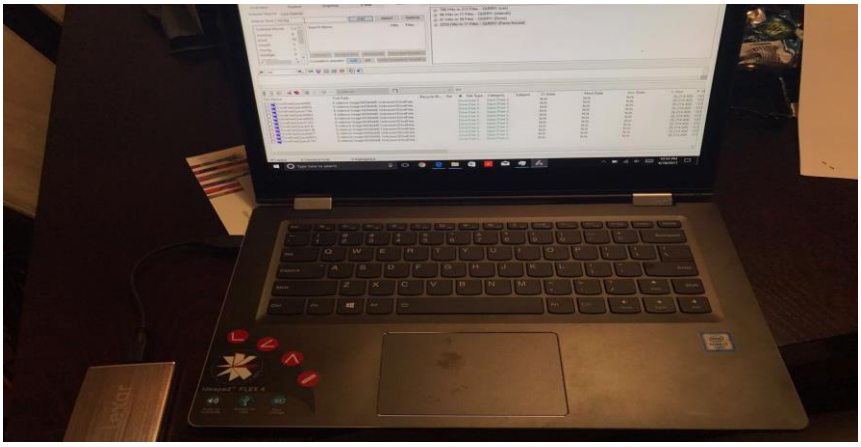

Figure 8. Lenovo Flex 4

A case involving some key evidence is designed and passed to both drives after they are formatted and wiped using HDShredder. Once evidence is passed on both drives it has been deleted and the drive is formatted. The random data is passed with evidence files in some combinations and without evidence files in some combinations. Drives are formatted after each combination made. The process is repeated for 8 times to make sure the evidence is destroyed completely and is not available for the forensic investigators.

Once the process is completed, a disk image is created for both the drives and it is passed through a forensic toolkit also known as FTK Toolkit to analyze the evidence. The evidence obtained from the hard disk drive is set as a hypothesis for this research and is compared to that of the results from a solid-state drive.

This paper involves comparison of evidence obtained from an HDD and SSD.

Tools and Techniques

Forensic Toolkit or FTK is a computer forensic software made by the access data. It helps in scanning the drive for various information. It can be used for locating deleted emails, scanning the disk for text strings for using them as password dictionary for cracking encryption. This

toolkit involves a standalone disk imaging program called FTK imager which is a simple but concise tool.

Hardware and Software Requirements

- FTK Toolkit
- HD Shredder
- SSD – Lexar 512GB LRWSSD512TBNA
- HDD – Seagate 1TB
- Laptop 1– Dell Inspiron 13 – I7359
- Laptop 2 – Len0vo Flex 4
- Instigator Laptop - Dell Inspiron 13 -7348
- OS – Windows 10 version

Figure 9. HDD – Seagate 1TB and SSD – Lexar 512GB

Literature Related to the Methodology

Forensic Analysis on SSD

Today's operations of SSD's allow only a little place for positive assumptions. The only assumption that can be made is that the investigator can get access to data that is being stored on the disk. Data that is being attempted to be destroyed, i.e., by formatting the disk in a quick format mode and the data which is being deleted normally would be lost forever within minutes. Even if the computer is being turned off immediately after a destruction command, i.e., quick format has been issued there is no way to stop the disk from destroying the data once the power is on. This resembles a situation like Schrodinger's cat which stated "No one is aware if the cat is alive until the box is being opened" (Schrodinger's cat, n.d.).

This resembles that the golden age of forensics is reaching an end. With the pace of development of technology in controller and SSD memory at an increase in the proliferation of the manufacturers and drives, it is probably never possible for removing or narrowing the new gray area within the forensic and legal domain. Scientists from Australia stated that "It seems possible that the golden age for forensic recovery and analysis of deleted data and deleted metadata may now be ending" (Bell, 2010).

Cannot delete. There are several design limitations that are being imposed by the way SSD drives are being constructed. The existing types of flash memories allow only a limited number of write operations before wearing off. Smart wear leveling techniques are being employed by the modern solid-state drives which instead of re-using the existing blocks of memory will write to a different block when the data that is being stored in a block is being modified. Due to this mechanism, the blocks which hold potentially sensitive information would be scattered all over the memory chip.

For increasing the life span and improving the wear leveling on solid state drives, many manufacturers are installing chips that can hold 25% more data than their advanced capacities. This additional capacity is not being addressable by means of the operating system, or by other reasonable means such as without usage of the custom hardware to access the flash chips directly. The contents of the solid-state drives cannot be wiped out securely as required by the military and government standards via traditional means due to the extra capacity (Belkasoft, 2014).

The implementation of an extension to ATA ANSI specification for enabling a secure destruction of information being stored on all flash drives to mitigate the issue is being done by some SSD manufacturers. The entire contents of the drive at hardware level are being wiped out by the correct implementation of the ATA secure erase SE command.

Software secure wipe tools will overwrite the information that is being stored on a hard drive with cryptographically secure random data in different passes. The main issue with these tools is their inability to address and access the entire storage capacity of a solid-state drive including the system, reserved, and remapped areas.

ATA secure erase command will instruct the built-in SSD controller supporting the command to electronically erase all the blocks on all the flash chips of the drive. The blocks would be completely empty and be available for immediate write if the SSD drives are cleaned effectively and completely, i.e., additional erase cycles are not required before writing information to write blocks. The SE command would restore the SSD to factory default and write performance. When the SE command is properly implemented, it would result in a complete wipe of all storage regions of SSD drive including any system, reserved and service areas (Domingo, 2015).

Cannot recover. Inability to recover the deleted data is another issue with the solid-state drives. The usage of wear leveling will result in excessive usage of the storage capacity of the drive, making use of a previously unoccupied block of data each time each write operation commences. Even a repeated write to the same file will cause the entire content of SSD drive to become "Dirty," which leads to a severe decrease in the performance with the write speeds being much slower than usual. This occurs because the flash technology that is being used in solid state drives would require the blocks to be erased before the controller can do a write operation on them. This property is unique to the storage drives that are based on flash technology and is completely different from how the traditional magnetic drives would handle the write requests.

The process of erasing the previous blocks that are occupied will be slower when compared to that of reading and writing. SSD, which is full of dirty blocks, would take significant time for writing even a single block of data as there are no empty blocks that exist. This made the SSD manufacturers design and develop a property named as garbage collection which would erase the dirty blocks in the background and would make them available for fast write operations again (Gubanov, 2012).

The problem with garbage collection process is that neither of the drives nor the controllers which control them have an idea of which blocks are being occupied by the files or operating system structures and which blocks are not being used and are dirty. The controller would mark the blocks that are being remapped to other blocks as a part of the wear leveling process. This information will only slow down the process of drive that is being filled with dirty blocks during the normal usage of the drive which involves writing, deleting, modifying, and creating.

For mitigating this issue, the SSD designers have developed an interface that allows the operating system such as Windows, Linux, Mac OS to let the controller know that certain blocks are no longer in use with the help of TRIM command. This would allow the internal garbage collector to erase the content of these blocks electronically and prepare them for future write operations (Wei, 2010).

SSD Self-Corrosion

Today's solid-state drives are destroying the court evidence by the process known as self-corrosion. Garbage collection that is running as a background process in most of the modern SSDs will erase the data permanently that is a market for deletion by removing it within a matter of minutes after data has been marked to be deleted. It is not possible for preventing the garbage collection by moving the disk to another PC or by attaching it to write blocking device. There is only a single possibility for preventing the self-corrosion, i.e., by physically detaching the disk controller from the flash memory chips storing the data and accessing the chips directly using a custom software (Memon, 2009).

Garbage collection. Garbage collection is the fundamental process in an SSD. It can be implemented in different ways that would impact the overall solid-state drive endurance and performance. Let us discuss in detail how garbage collection works, way it can be implemented and how is it related to TRIM command and over provisioning.

Hard disks can overwrite data, but the NAND flash memory cannot do the same. The old data must be erased first before a new data can be written to the same location. In an SSD, the process of the changing or relocating the existing data to a new location and allowing the surrounding data that is invalid o be erased in an SSD is known as Garbage Collection (Eleftheriou, 2009). The flash memory is divided into blocks which are further divided into

pages. Data can be written into an empty page, but the whole blocks need to be erased. So, for reclaiming the space that is taken up by the invalid data, all the data that's valid in that block must be copied first and written into empty pages of the new block. Only then, the data that is invalid in the original block can be erased for making it available or ready for new data to be written.

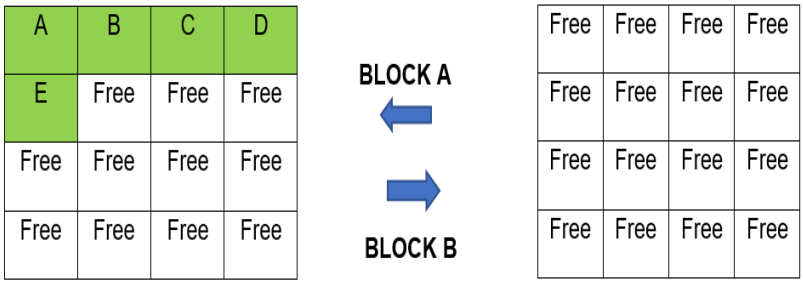

Figure 10. Garbage Collection Process, Initial Allocation

The Garbage collection process can be simply explained using the help of a diagram. Consider the Figure 10 above. Block A and Block B are two different blocks in an SSD. Pages A-E are written with information in Block A and Block B is completely empty and is ready to be written. Sometime later, the data is being changed, so the pages A-E are written and the original pages A-E are being marked as invalid, i.e., shown in the figure below. At the same time, additional information has been written to pages F-K. So, the Block A is full but it is still holding space for the invalid data in A-E, which cannot be reclaimed until the complete block is being erased.

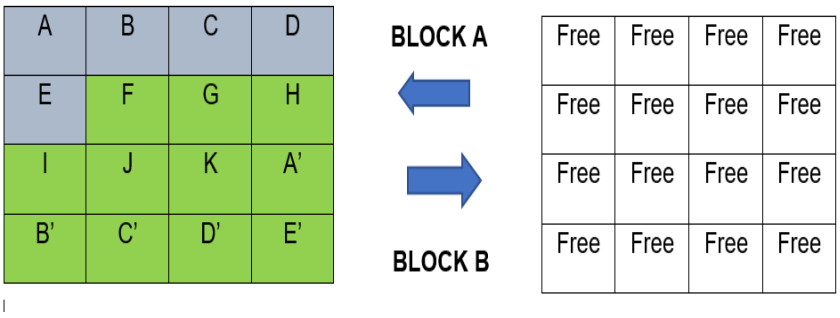

Figure 11. Garbage Collection Process, Adding Data

For achieving this objective, the valid data in Block A must be moved to a new block so that the original block can be erased and new data can be written. The figure below shows that the data from pages A-E along with the data from F-K is being written to a new Block B so that the space in Block A can be reclaimed by erasing the data.

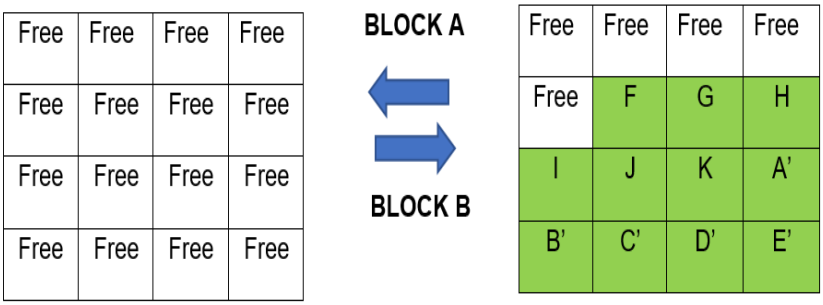

Figure 12. Garbage Collection Process, Moving Data to a New Block

The writes from this step are not done by the host system and are the source for increasing the write amplification in a solid-state drive which means that the flash in an SSD is being written more than what came from host originally. Since the flash memory has a limited number of write and erases cycles, this operation should be minimized whenever possible however it is a necessary part of an SSD's operation (Smith, 2011).

Wear leveling typically occurs during the garbage collection as the data is being written to a variety of new blocks to spread wear around over the breath of solid state drive. Since the

flash can sustain a limited number of writes over a lifetime, and if the data is always written to the same block, then its life of write cycles will be exhausted prematurely when compared to other blocks. This early block retirement would result in a decrease in the storage capacity of the drive and prevents it from performing at full capacity. Ideally, all the block of the SSD would need to be worn at the same rate throughout the lifetime of the drive.

Operating System Awareness vs. Drive Awareness

In an HDD, the operating system can simply request the new data to be written to the same location where the older, i.e., the invalid data is being stored and the HDD can directly overwrite the old data. However, when compared to an SSD, the data must first be erased before it can be written to locations that previously hold data as the SSD cannot directly overwrite the existing data as stated earlier.

The operating system understands the files and their structures also the logical locations where they are being stored but it cannot understand the physical storage structure of the storage device. The storage device in any storage system does not know the file structure, it just knows that there are bytes of data being written in specific sectors. The storage system, i.e., the SSD or HDD will return the data from the physical location when the Operating system would ask for the data in corresponding logical locations (Lal, 2009).

When an operating system deletes the file, it will simply mark the space that's being used for that data as free in its logical data table. In an HDD, there is no necessity for the operating system to let the storage device know about the deletion as it would simply write something new into the same physical location in future. Wherein the case of an SSD, it becomes aware that data is being deleted only when operating system tries writing to that location again. Now SSD marks the data that is invalid or the old data and it starts writing new data to a new physical location. It

may also perform garbage collection at the same time; however, it varies between SSD architectures and other conditions at that moment.

The TRIM Command

The newer operating systems for example, Windows 7, Linux 2.6.33, Windows Server 2008 R2, Mac OS X Lion, FreeBSD 8.2, Open Solaris, TRIM command will enable the OS to notify that the SSD which contains the old data is no longer valid about the time it deletes the logical block addresses from the logical table. The advantage of the TRIM command is that it will enable the Garbage Collection of SSD to skip the invalid data rather than moving it, this would save time not rewriting the invalid data. This helps in the reduction of a number of erase cycles on flash memory and would enable higher performance during the writes. The SSD does not need to garbage collect these or immediately delete these locations, it can just mark them as no longer invalid (Belkasoft, 2014).

The differences are illustrated in the figure below.

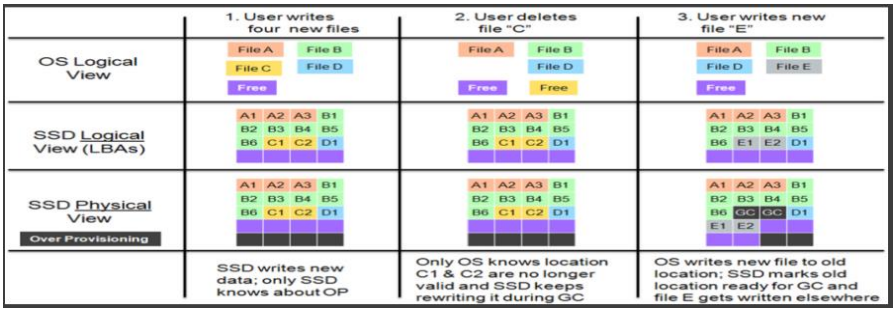

Figure 13. Garbage Collection without TRIM Command (Tokar, 2012)

The process shown above is without the TRIM command in use. The SSD user writes four new files to the drive. OS sees the new files in the logical table, SSD will have both the logical and physical view of space available, which in physical view includes over provisioning space which is not part of drives stated capacity as known to the operating system. Users delete

File C in Column 2 but the system is not aware that the file has been deleted because TRIM command is not in use. If garbage collection is done at this point, then it will move the invalid data in File C as it does not know that it is invalid. In Column 3, SSD will write a new file to the free space making the old space from File C as available for Garbage Collection (Tokar, 2012).

The figure below illustrates the difference with TRIM command. The process is the same when a user writes four original files. When the user erases the File C, it is marked invalid immediately in the preparation for garbage collection as the OS uses the TRIM command. Space which originally holds the File C is now a free space and becomes available as a dynamic over provisioning meaning that SSD has more free space during the garbage collection which helps in improving the overall SSD performance. When a user finally writes the File E, the total space on the SSD is same as the drive without TRIM. The difference is that SSD with TRIM support knows that the data is invalid and it can be considered free space during the garbage collection and prevents the moving of invalid data to another block.

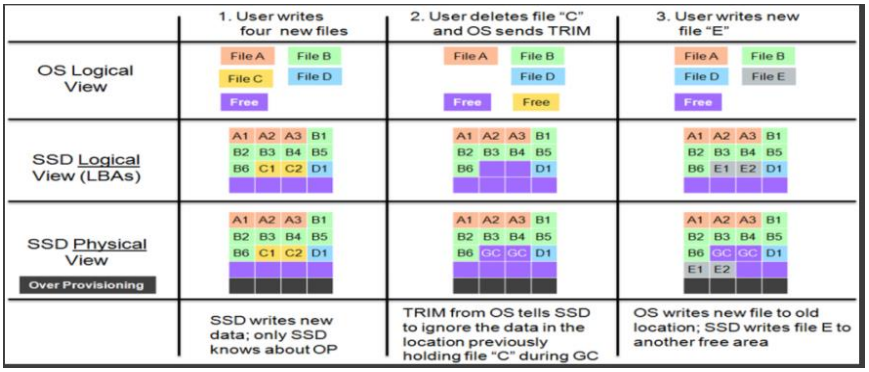

Figure 14. Garbage Collection using TRIM Command (Tokar, 2012)

Wear Levelling

As the number of available spare blocks in a flash drive storage device is limited, there is a need of special flash management techniques to overcome and manage the flash wear out

phenomenon. One of such technique is known as wear leveling. Wear leveling helps in even out erase programs or distribution of program on all the available blocks on a flash drive. This is done by writing to a new free block with all new or updated data and then erasing the block with old data and making it available within the free block pool. The wear leveling operation is completely transparent to the host system as it is done in the background (Corsair, 2007). There are two methods used for wear leveling namely static and dynamic wear leveling.

Dynamic wear levelling. Dynamic wear leveling works with data blocks that are being written dynamically. As mentioned earlier the data is written to the free data blocks, i.e., the blocks which do not contain user data. Flash drive controller will select the new free data blocks based on the erase cycles that the blocks earlier had. Once the data is written, the controller would update its internal logic to the physical mapping table to point to new physical block location. Data block containing the old data is being marked invalid and it is then erased and made available as a new free block during the garbage collection process. Dynamic wear leveling will address the issue of repeated writes to same blocks by redirecting the new writes to a different physical block thereby avoiding the premature wear out of the actively used blocks (Handy, 2012). The following diagram explains the dynamic wear leveling process.

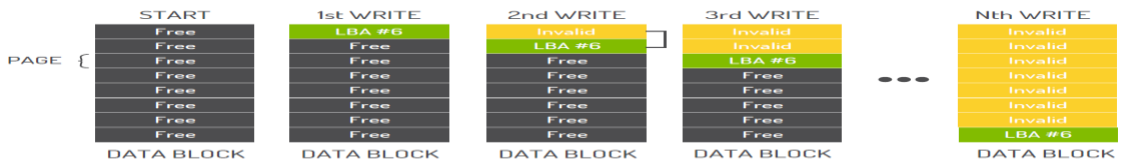

Figure 15. Dynamic Wear Leveling Process (Cactus, 2014)

Figure 16. Garbage Collection in Dynamic Wear Leveling (Cactus, 2014)

Static wear levelling. In contrast to the dynamic wear leveling, static wear leveling will level all the data blocks including those which are not written to. This process is done in the background and it completely transparent to the host system. Different vendors have different mechanisms for triggering the static wear leveling operation (Handy, 2012).

For example, let us consider one such trigger could be a difference in the program or erase counts between the blocks in the static data pool and the blocks in the free pool. When the threshold level is being triggered, then the block in static data pool with the lowest erase count will be swapped with the block in the free data pool with the highest program or erase count. The following diagram is the conceptual implementation of the example.

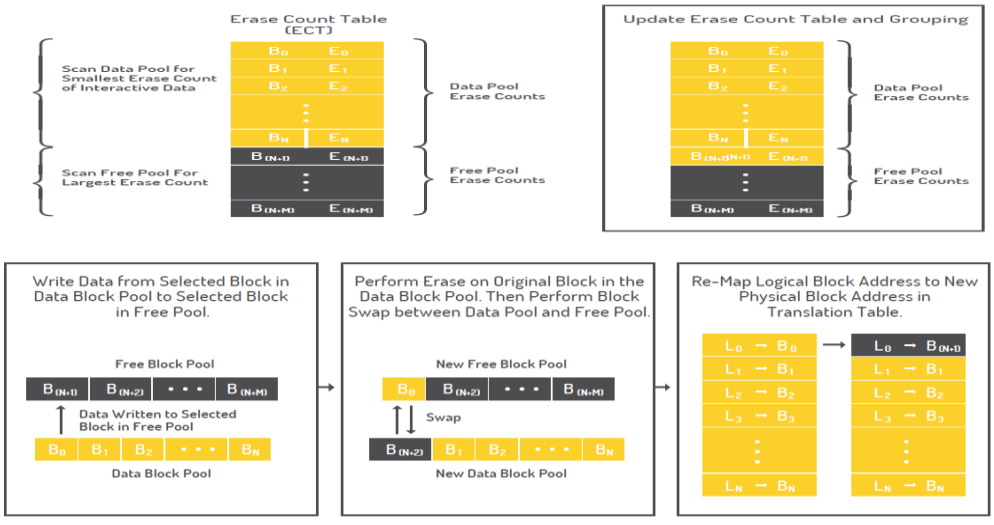

Figure 17. Conceptual Implementation of Static Wear Leveling Process (Cactus, 2014)

Summary

In this chapter, we discussed the tools required, hardware and software requirements for conducting the experiment. The special features in an SSD which makes it difficult for forensic investigators to capture the evidence such as wear leveling, TRIM, garbage collection and the collection method, design of the study is being discussed. In the next chapter, we will be discussing of how data is being presented and analysis is being done.

Chapter IV: Data Presentation and Analysis

Introduction

In this chapter, we will discuss how data is collected, how data is being passed on both the drives, how we are going to compare and analyze the results obtained from both the drives. We will discuss how the tools are being used in gathering the images from the drives, how drives are being formatted and wiped to erase the data, and analyze the evidence folder when it is passed through FTK Tool kit.

Data Presentation

The data collected is a combination of word documents, images, pdf files and information in notepad. For comparing the results using some keywords, the evidence files are created of five different files named as a car, dose, farm house, islands, and mortgage. Each file has data that are related to the file name. For example, the car folder has images of 10 different cars chosen at random and four notepad documents which have information regarding car manufacturers and dose folder contains 10 images of vaccines and four-word documents. Following are the contents of individual evidence folder.

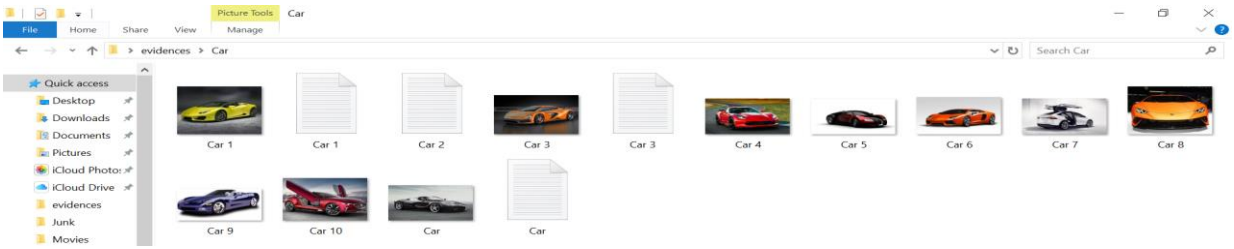

Figure 18. Contents of Car Folder

Figure 19. Contents of Dose Folder

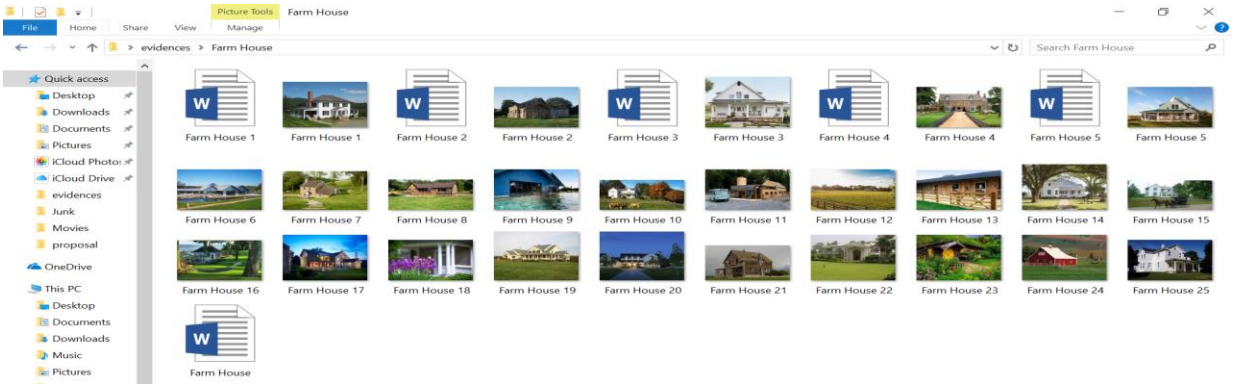

Figure 20. Contents of Farmhouse Folder

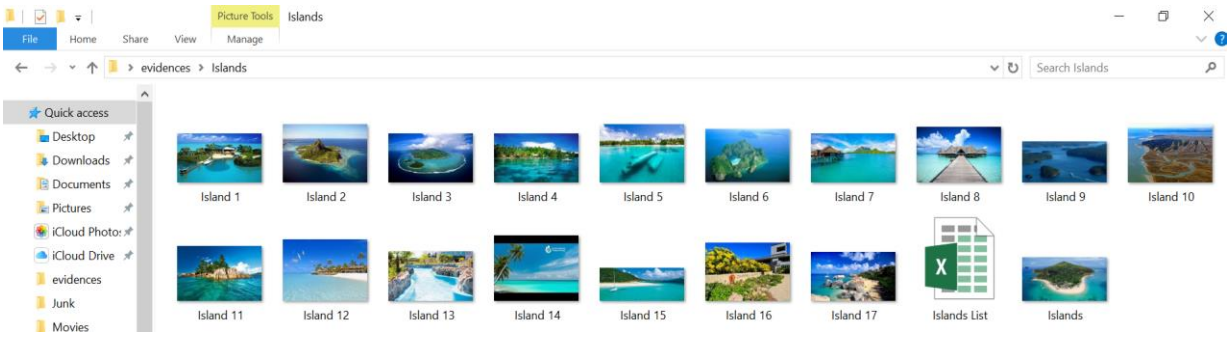

Figure 21. Contents of Islands Folder

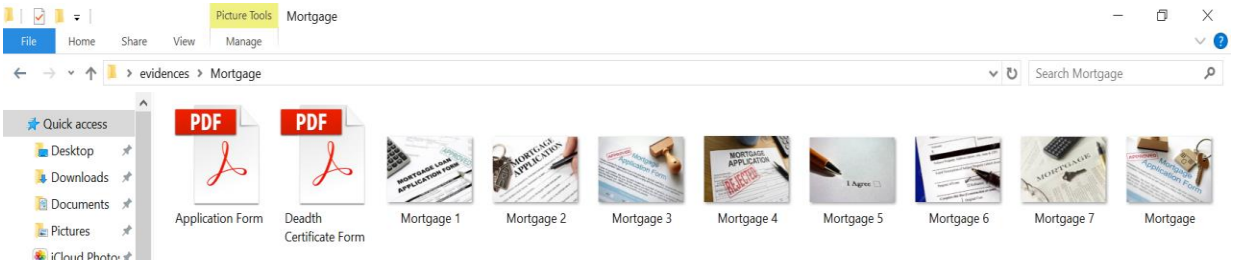

Figure 22. Contents of Mortgage Folder

Evidence was first passed to Both HDD and SSD and was deleted. Four Evidence Trasher files were created and a Junk File folder which has multiple Word Documents, Excel Sheets, PDF Files, and Images. All these evidence Trasher files were 100 GB together in size.

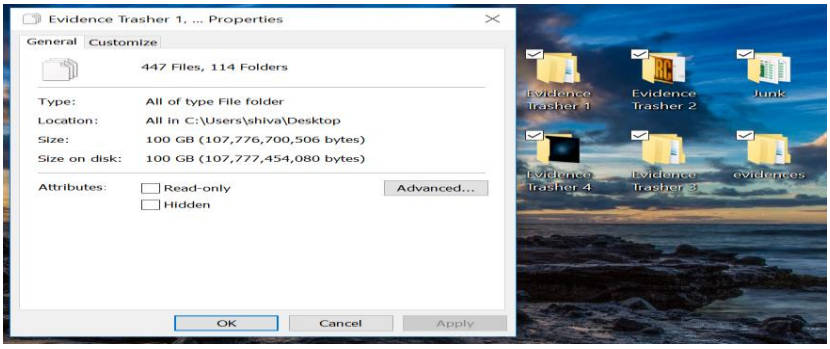

Figure 23. Combined File Size of the Evidence, Evidence Thrashers, and Junk File

Both SSD and HDD are wiped using HDShredder. Even though both the drives that are being used for this experiment are brand new, just wanted to make sure there is no data present on the drives earlier.

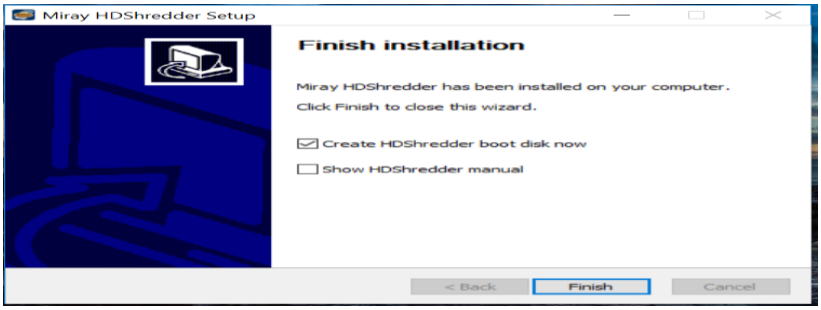

Figure 24. Installation of HD Shredder

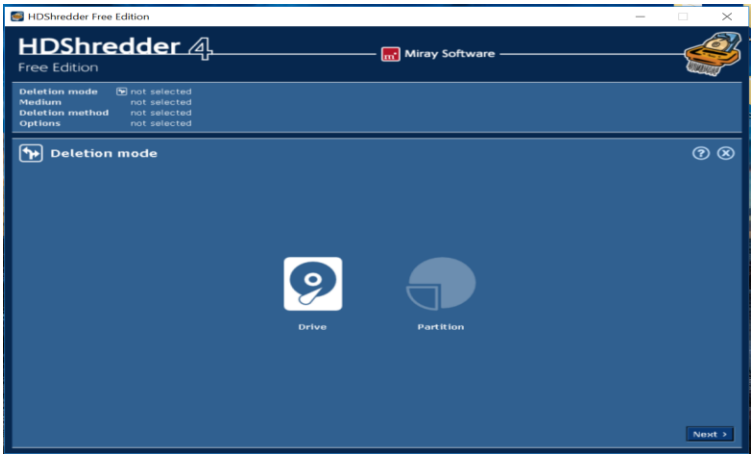

Figure 25. Running HD Shredder

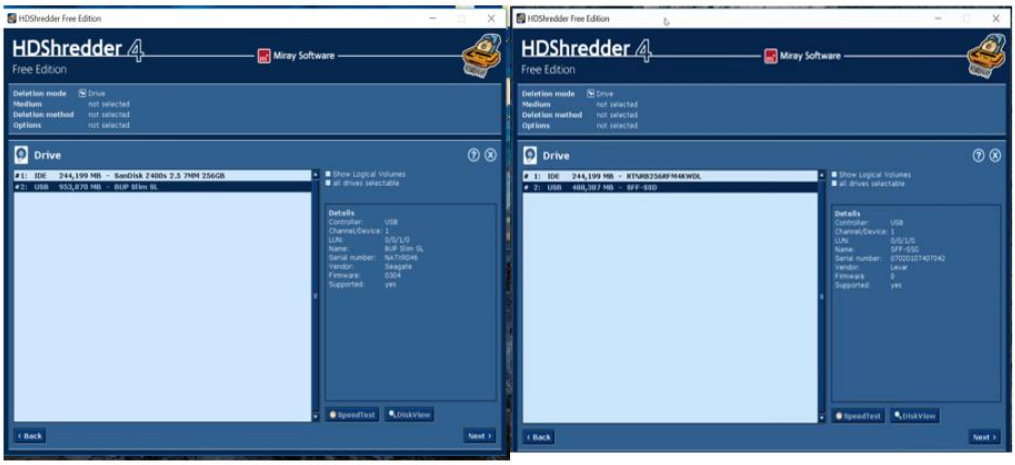

Figure 26. Detecting Both the Drive on Two Different Laptops

Once the process is initiated it took around three hours for the drives to be completely wiped using the HD Shredder software.

Figure 27. Drive Wiping Process at Random Intervals in HDD and SSD

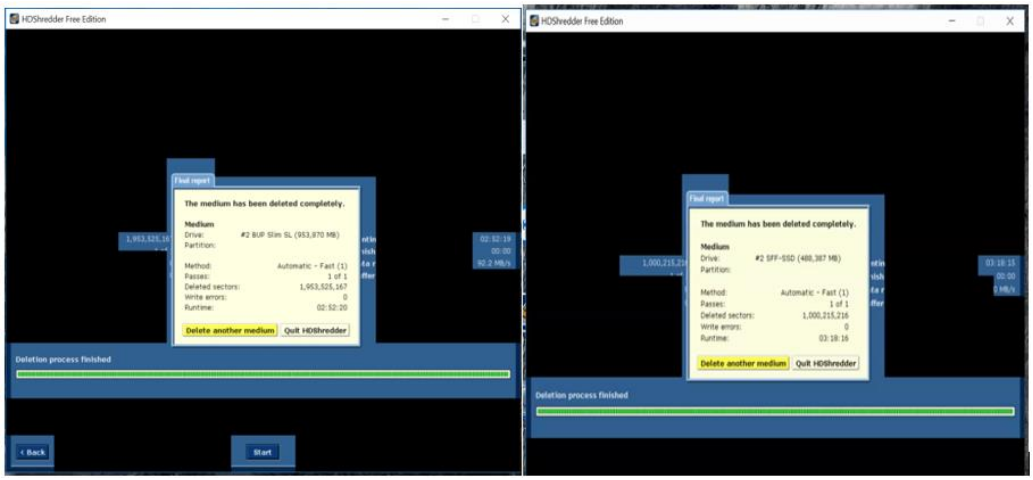

Figure 28. Successful Completion of Disk Wiping using HD Shredder

All the evidence trasher files are passed to both HDD and SSD at different combinations. The following figure illustrates the different combinations that are being used.

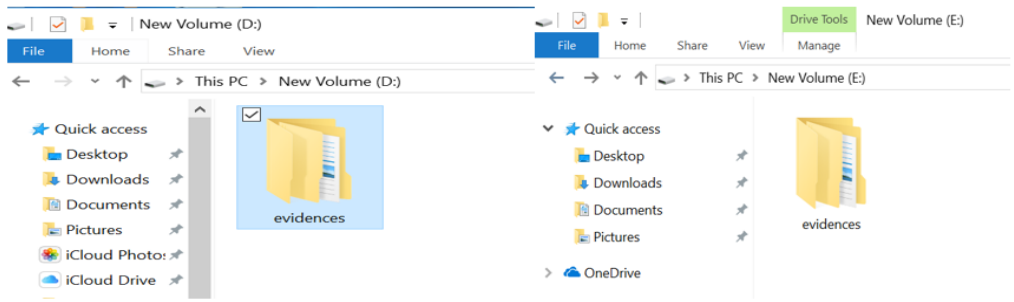

Figure 29. Passing Evidence and Deleting in HDD and SSD

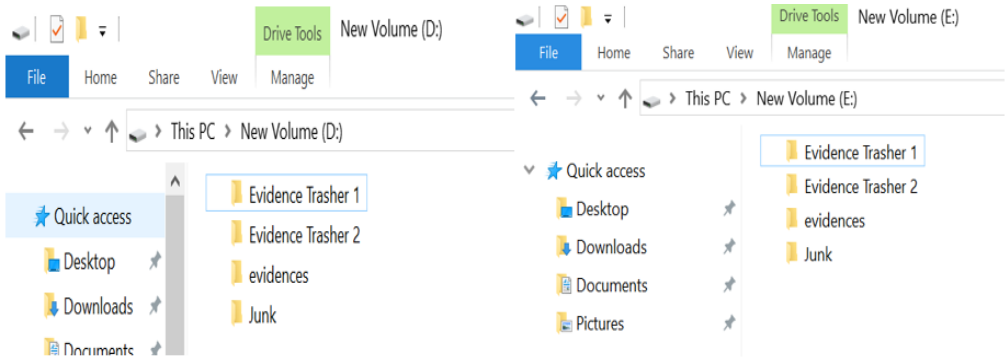

Figure 30. Passing Evidence Trasher 1, Evidence Trasher 2, Junk File, and Evidence and deleting in HDD and SSD.

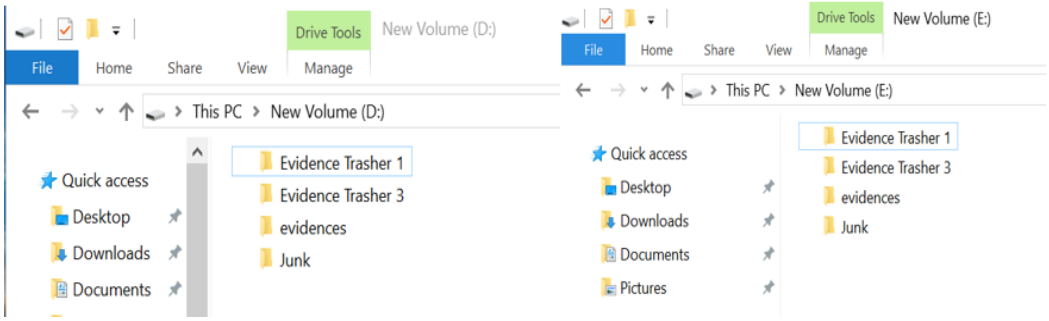

Figure 31. Passing Evidence Trasher 1, Evidence Trasher 3, Junk File, and Evidence. Deleting Previous Files and Deleting in HDD and SSD.

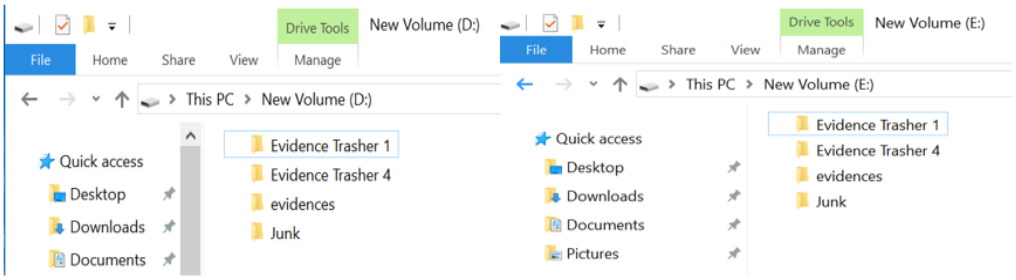

Figure 32. Passing Evidence Trasher 1, Evidence Trasher 4, Junk File, and Evidence. Deleting Previous Files and Deleting in HDD and SSD.

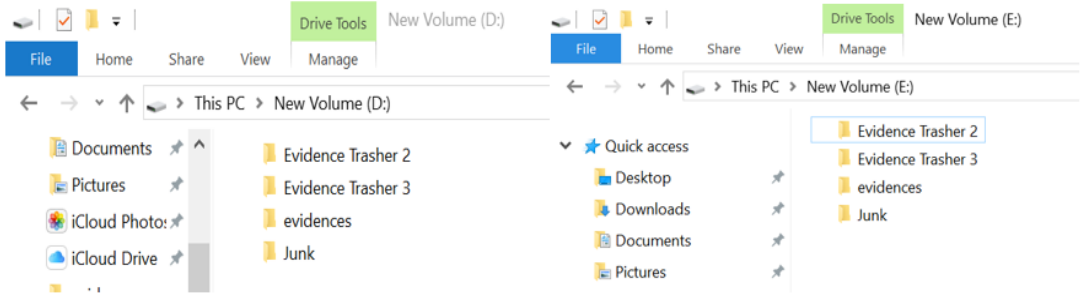

Figure 33. Passing Evidence Trasher 2, Evidence Trasher 3, Junk File, and Evidence. Deleting Previous Files and Deleting in HDD and SSD.

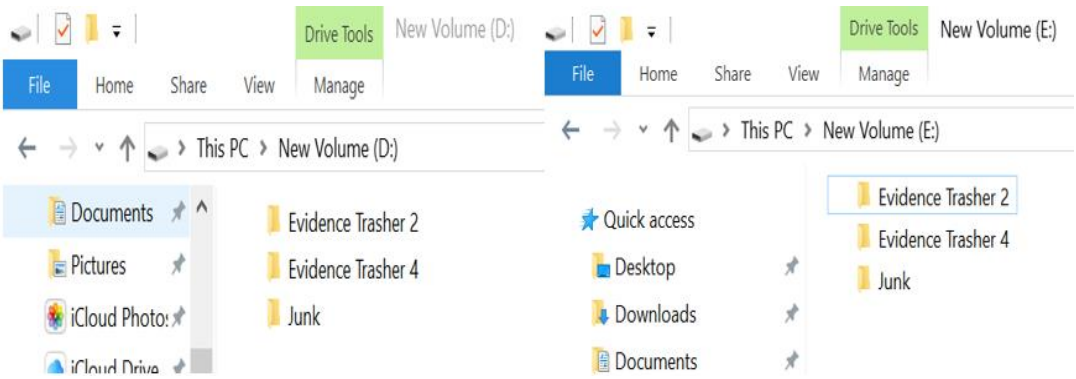

Figure 34. Passing Evidence Trasher 2, Evidence Trasher 4, and Junk File. Deleting Previous Files and Deleting in HDD and SSD.

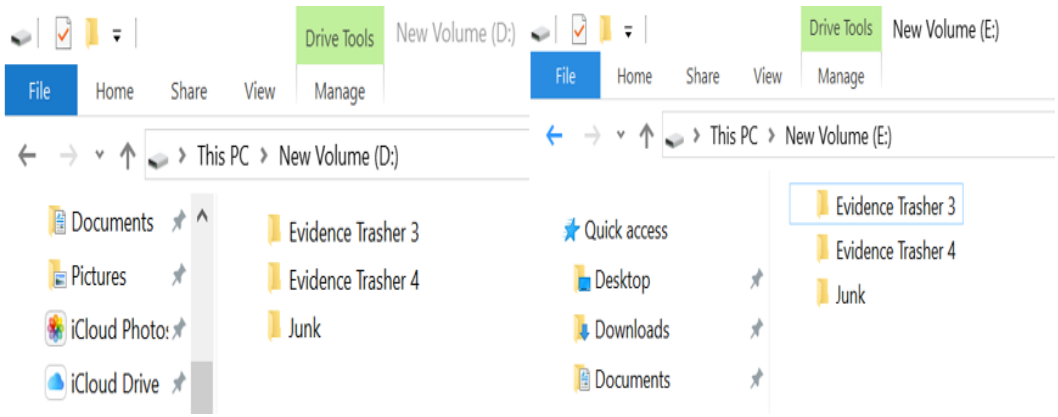

Figure 35. Passing Evidence Trasher 3, Evidence Trasher 4, and Junk File. Deleting Previous Files and Deleting in HDD and SSD.

After the completion of all these combinations, the process is being repeated for 8 times by changing the order of combinations and disks are being formatted each time combinations are done.

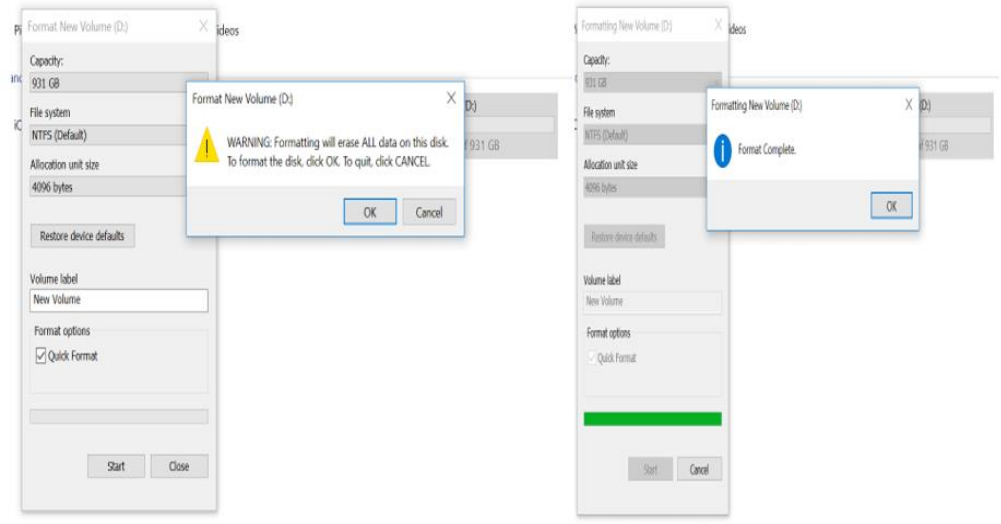

Figure 36. Formatting Disk after Data is Being Transferred in HDD

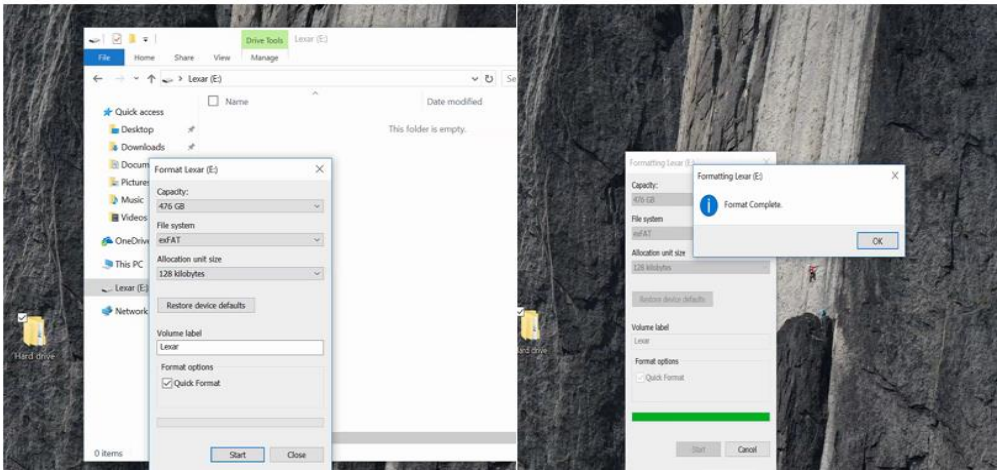

Figure 37. Formatting Disk after Data is Being Transferred in SSD

Creating an Image of the Evidence folder to analyze the contents of the folder in FTK.

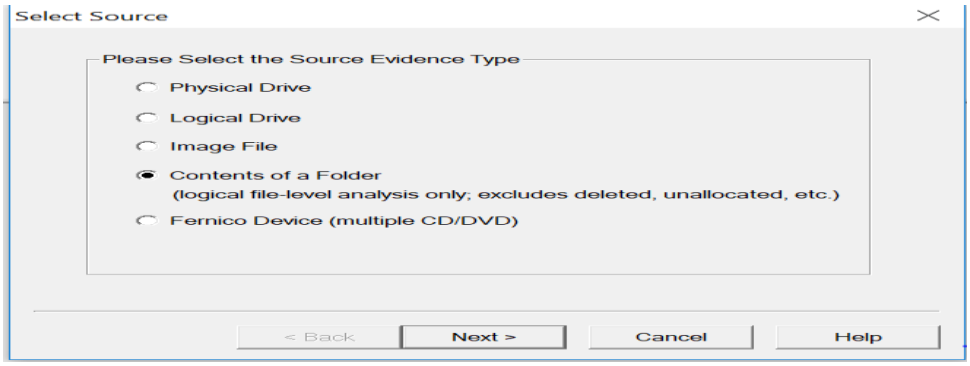

Figure 38. Selecting the Source Evidence as Contents of a Folder

As we are selecting contents of a folder, it does not include any metadata, deleted files, unallocated space, etc. in the image created. Following is the warning displayed.

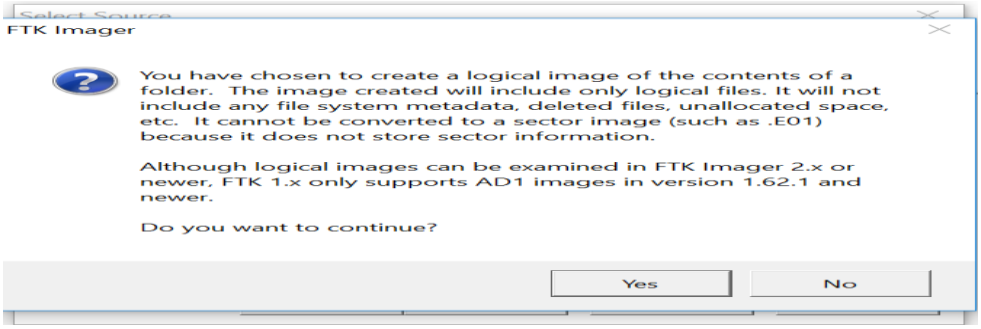

Figure 39. Checking Conditions before Creating the Image of a Folder

It prompts to select the folder for which an Image needs to be created. Using browse we select the source path.

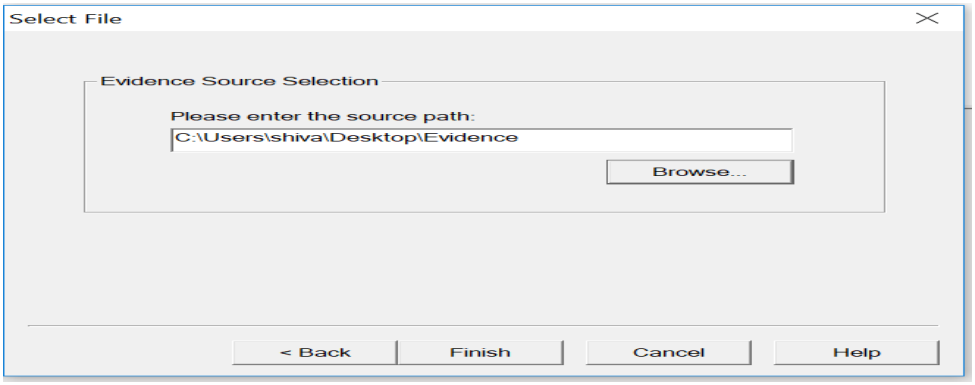

Figure 40. Selecting the Source Path for Image of Folder

A random data is given for case number, evidence number, examiner, and unique description.

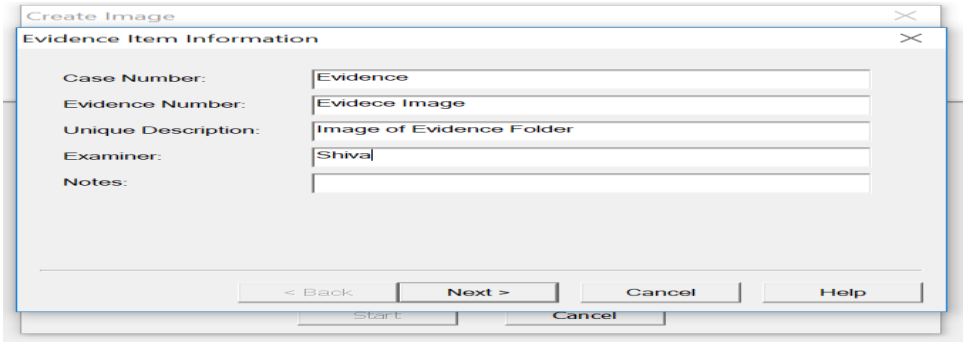

Figure 41. Assigning Name for Unique Identification

The image source is selected as the evidence folder on the desktop and destination is provided as the desktop of the same computer being used.

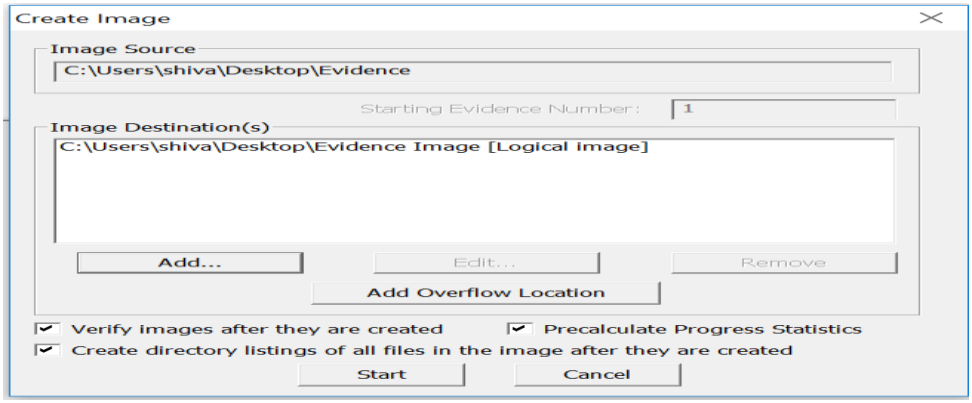

Figure 42. Assigning Image Destination for Image of Evidence Folder

Image destination and fragmentation size can be modified in this step. If we are dealing with a huge file, then we can change the fragmentation size for better results.

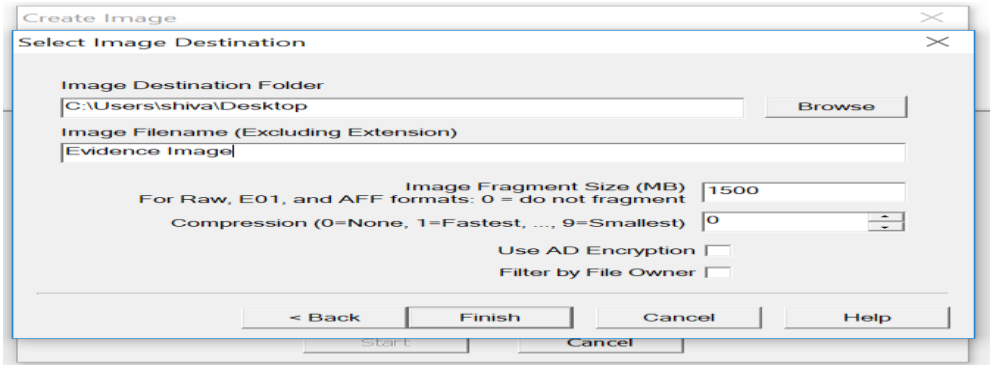

Figure 43. Selecting the Fragmentation Size for Image of Evidence Folder

We can monitor the progress of the Image creation as shown below. As the image creation is for a single folder, it does not involve any metadata, deleted files etc., the processing time required is very low because it acquires the image of content in the folder.

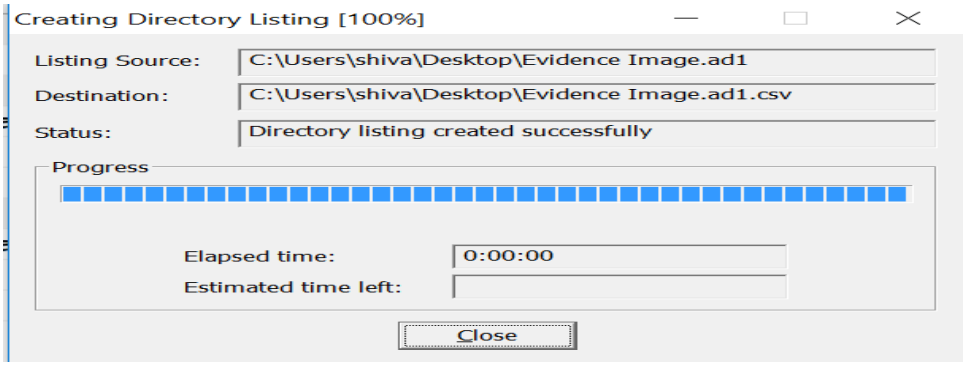

Figure 44. Processing of Image Creation for Evidence Folder

After successful completion of Image creation, a Results window is displayed as shown below.

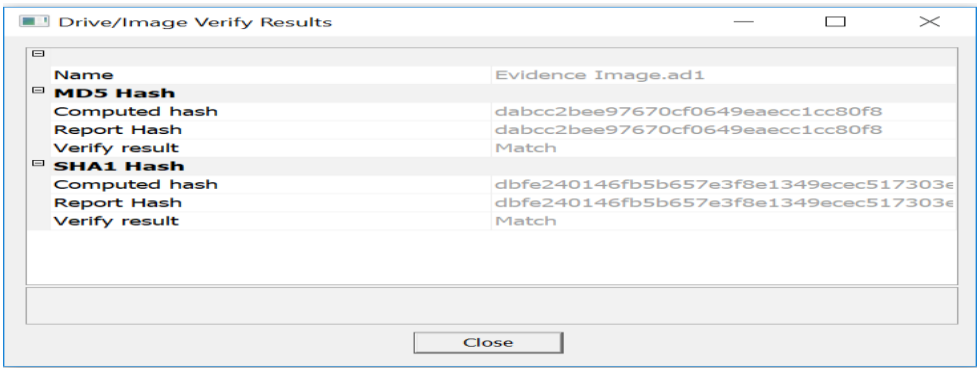

Figure 45. Verifying Results of the Image Created for Evidence Folder

Image summary gives you a brief information of the image created such as case number, name, start time, and end time.

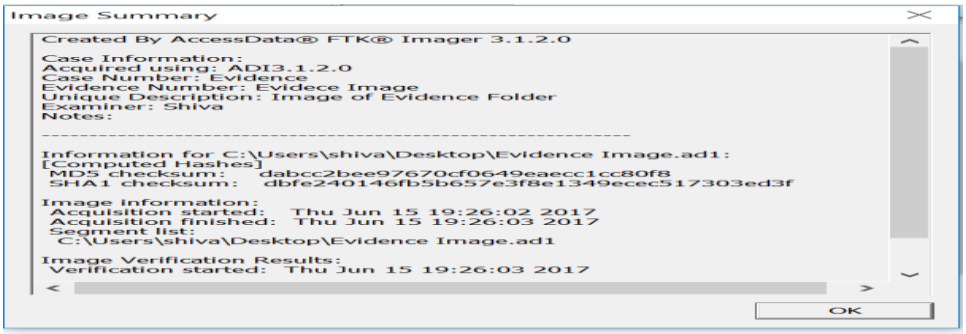

Figure 46. Image Summary for Image of Evidence Folder

Once the image is created, it is stored at the location which is assigned during the image destination folder selection steps. In this case, we selected it to be a desktop, so the image is stored on the desktop as shown below.

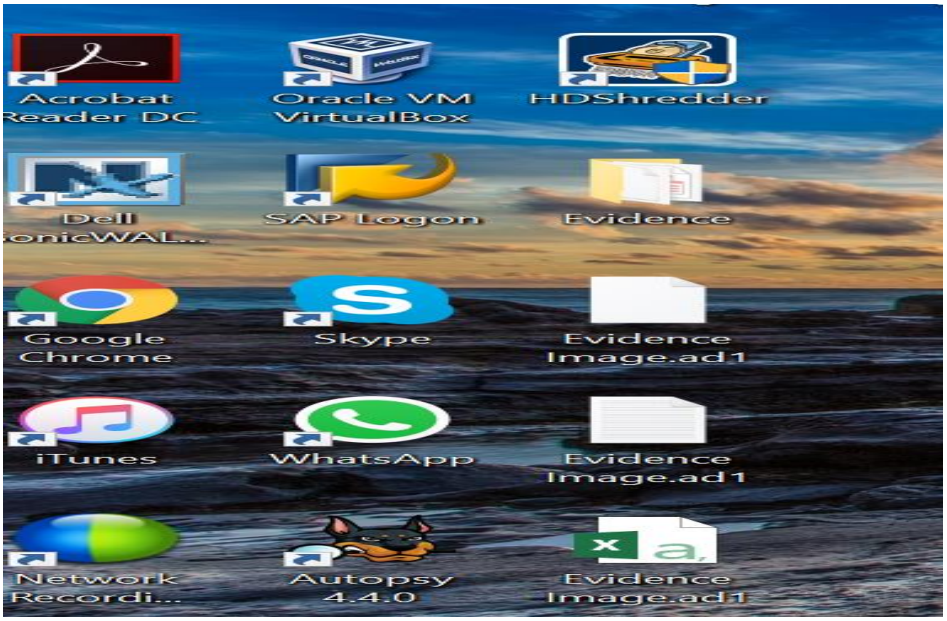

Figure 47. Image of Evidence Folder Stored on Desktop

Data Analysis

After successful completion of Image creation, the image of the evidence is being analyzed using FTK Toolkit. In the previous section, we have created an image for the evidence folder. Now we will analyze the image created using FTK Toolkit.

Analyzing the Image of Evidence Folder

To analyze the image created using the FTK Imager, we will use FTK toolkit. During the starting of analyzing the image, we will be asked to provide a case number, name, and select a path.

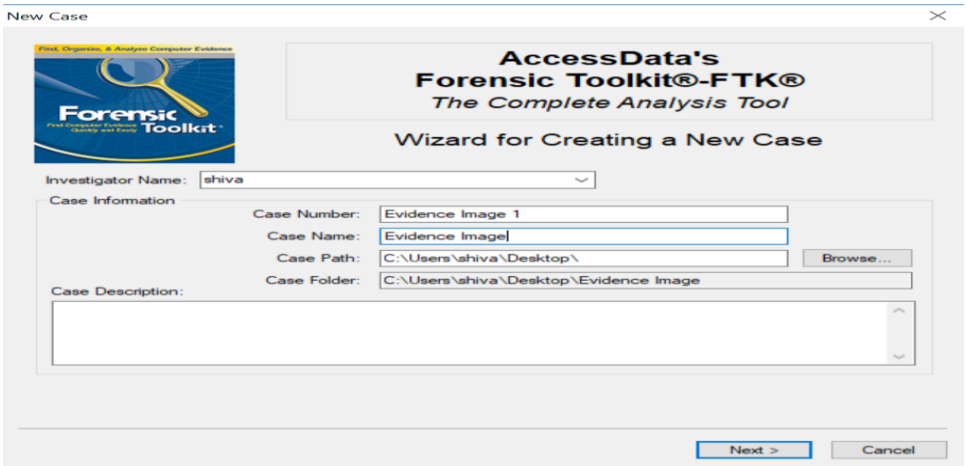

Figure 48. Assigning Case Name for Analyzing the Evidence Folder

In the next step, we will be asked to enter some demographic information such as the name of the examiner, address, email address, phone number, etc. A random data can be given for the same. The information furnished here will be shown in the report that will be generated once the image extraction is done.

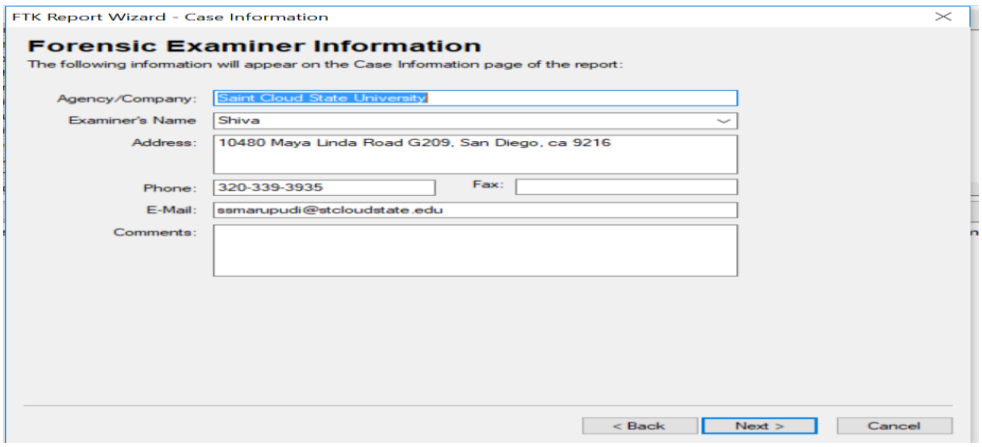

Figure 49. Filling Demographics for Evidence Folder

In the next step, we need to choose the evidence image that needs to be analyzed. As the image is already acquired we will be selecting the acquired image of the drive.

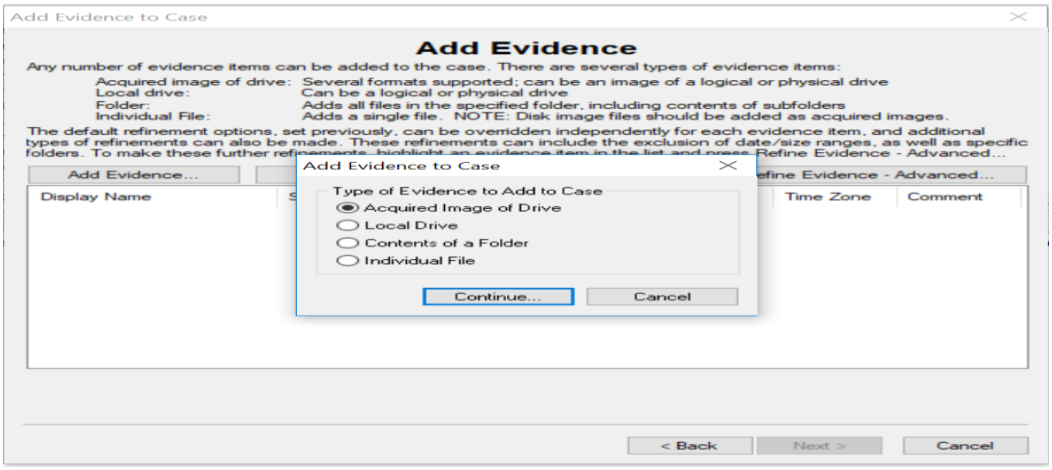

Figure 50. Adding Evidence to FTK Toolkit

Now, select the image of evidence folder from desktop and assigning a name for display.

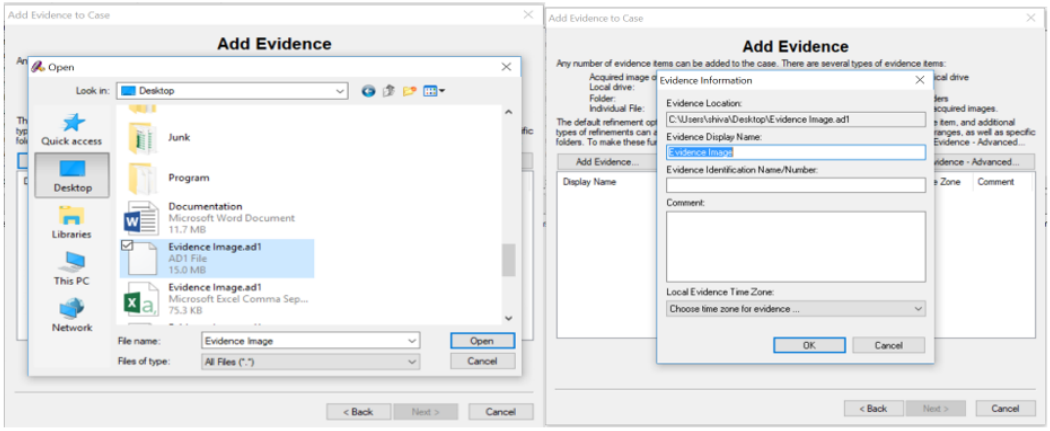

Figure 51. Adding Evidence and Assigning Name for Analyzing Evidence Folder

In the next step, the evidence file selected is being displayed followed by setup complete dialogue box.

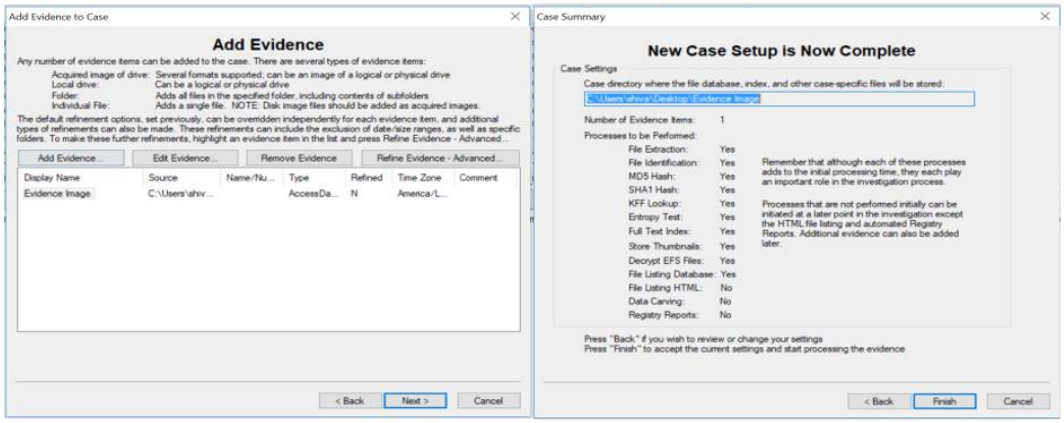

Figure 52. Verifying Evidence Selected and Completing the Setup for Evidence Folder

A window showing that the files are being processed appears as shown below.

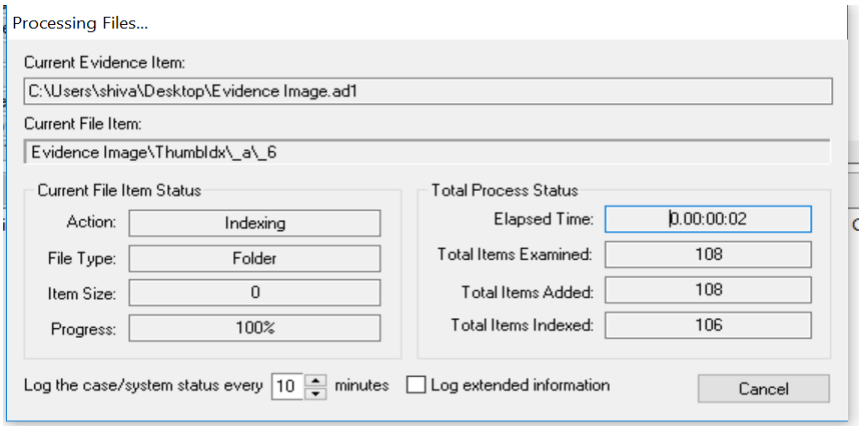

Figure 53. Extracting the Files from Image of Evidence Folder

Once the processing is completed, the image is ready to be analyzed and it is shown in FTK Toolkit.

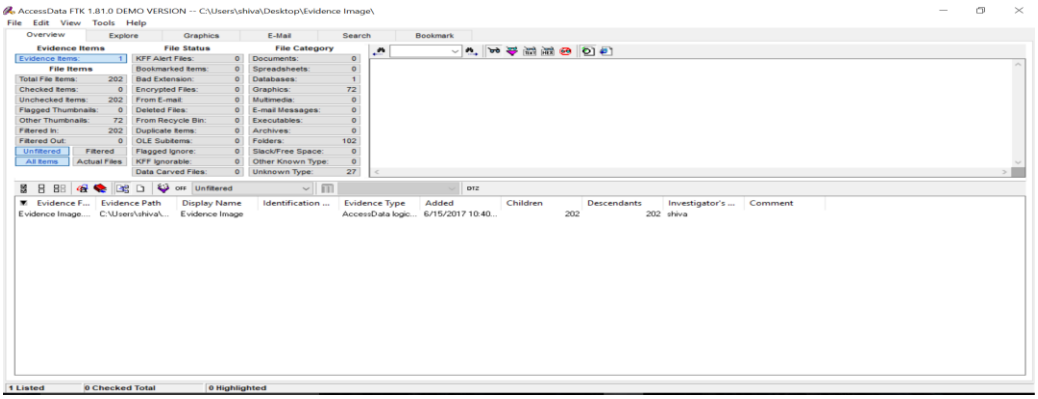

Figure 54. Analyzing the Image of Evidence Folder in FTK Toolkit

The analysis is done by searching the keywords. In the evidence folder we created, we used five different keywords such as car, dose, islands, farmhouse, and mortgage. So, we search for these keywords in the evidence extracted. Following are the results that were obtained from the keyword search.

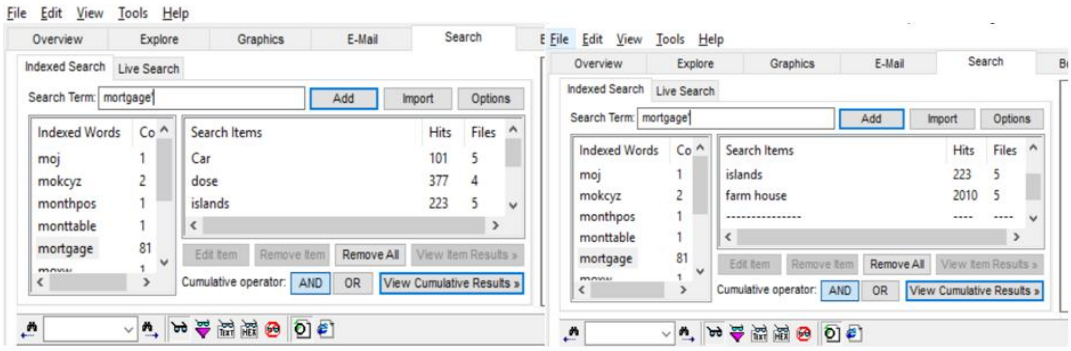

Figure 55. Results Obtained Using the Evidence Folder Image

We can also look at the images, word files by selecting the respective file names which we are aware of. From the evidence folder, we are aware that there is a picture of a farm house. So, with the respective jpg file name, we can just click on it and obtain the respective image. The forensic investigator will search each file to know what is the content of the file.

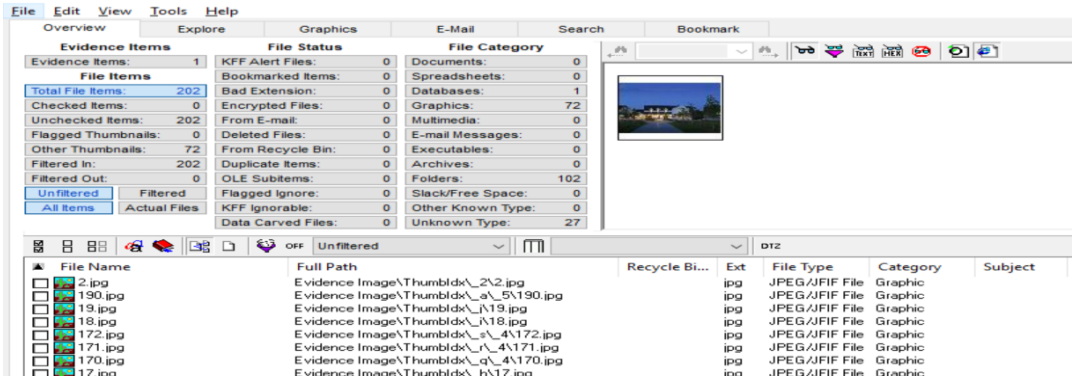

Figure 56. Searching by the File Names in the Image of Evidence Folder

In a similar manner, the results obtained from both SSD and HDD are compared based on the files recognized and the number of hits. After the successful analysis of all the images of both the disk, we will use the quantitative research approach and prepare a table of the files that were able to be identified even after deleting the evidence and formatting the disks individually. Comparing the files identified will help us understand how the special features designed in an SSD are being to destroy the evidence and make it difficult for the forensic investigators.

Summary

In this chapter, we discussed how the image evidence file is being created and how it is being analyzed using the FTK Toolkit. In the next chapter, we will create an image of HDD and SSD, analyze the results by comparing the results obtained by searching the keywords in both the HDD and solid-state drive.

Chapter V: Results, Conclusion, and Recommendations

Introduction

In this chapter, we will discuss how the images of both HDD and SSD are created, analyzing the images using FTK Toolkit and finding the number of files, hits identified for the key searches and compare the results of both HDD and SSD.

Results

Creating Image of HDD

In the process of creating an Image of the HDD, we use the option of the Logical drive which helps in selecting the drive in specific or, if we want to create an image of the disk on the laptop you are using, then we can use the physical drive and select the drive that is being installed in the system. The laptop used for creating the HDD image has only a single drive of 256 GB named as C drive.

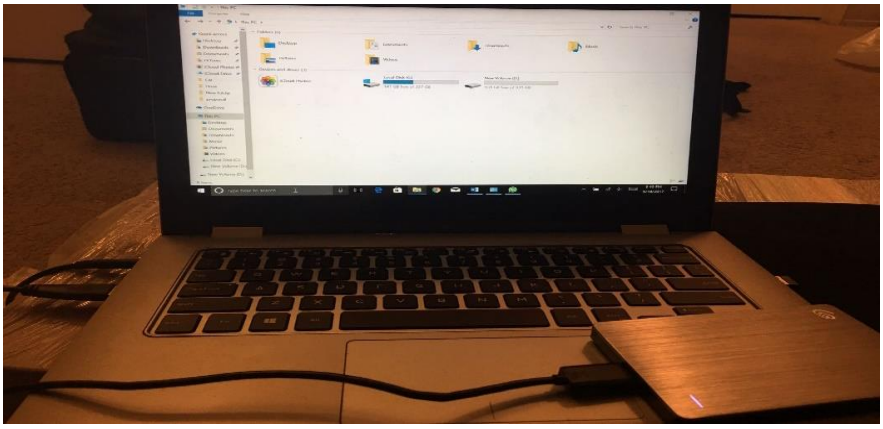

Figure 57. HDD Connected to Laptop 1

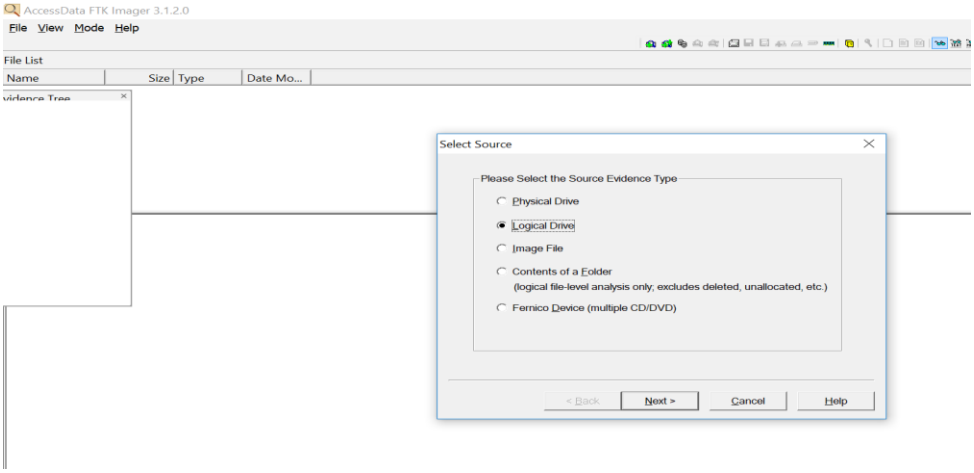

Figure 58. Selecting the Logical Drive for HDD Image Creation

The HDD drive which is being used to analyze is D drive attached to the laptop. So, we will select D drive in the next step.

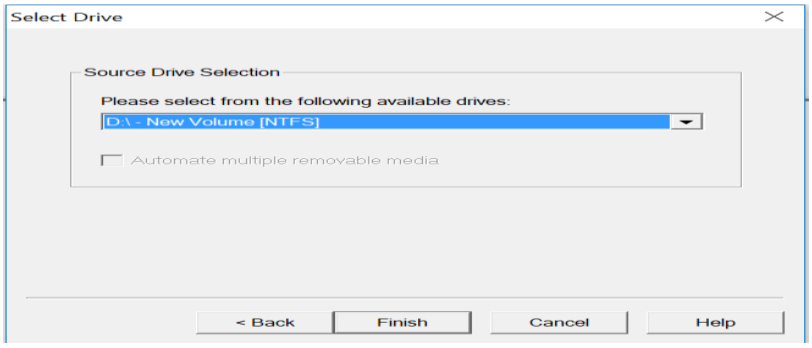

Figure 59. Selecting HDD Drive for Image Creation

Like the image creation of folder, we need to add the destination of where the image needs to be stored. As the drive is of the large size of 1TB, the image destination is selected as D drive.

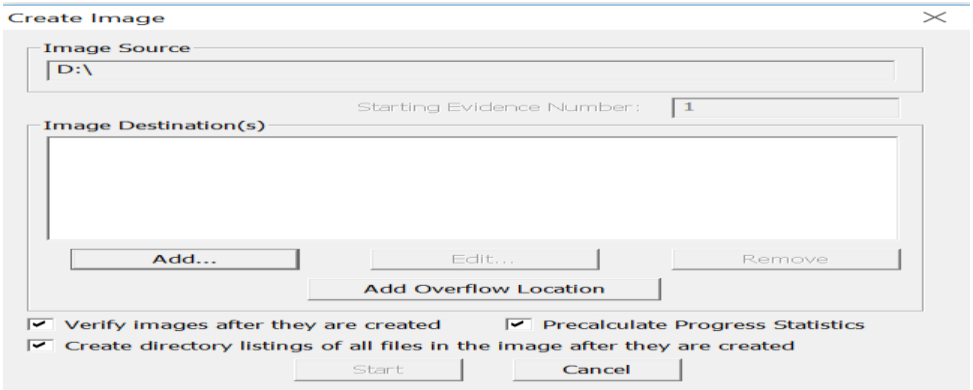

Figure 60. Selecting the Destination for Image of HDD

Unlike the folder, disk image has an option of Raw, Smart, E01 and AFF format of the image. We will use the Raw image.

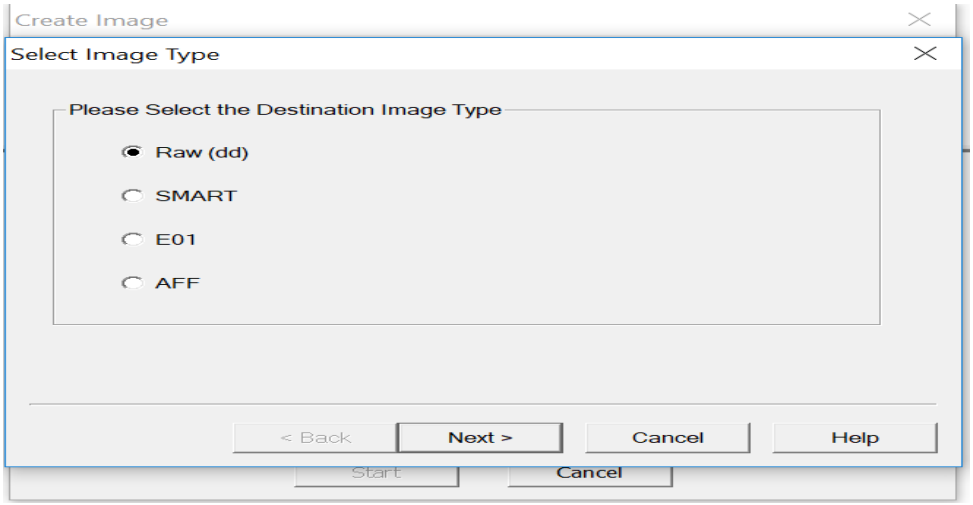

Figure 61. Selecting the Type of HDD Image

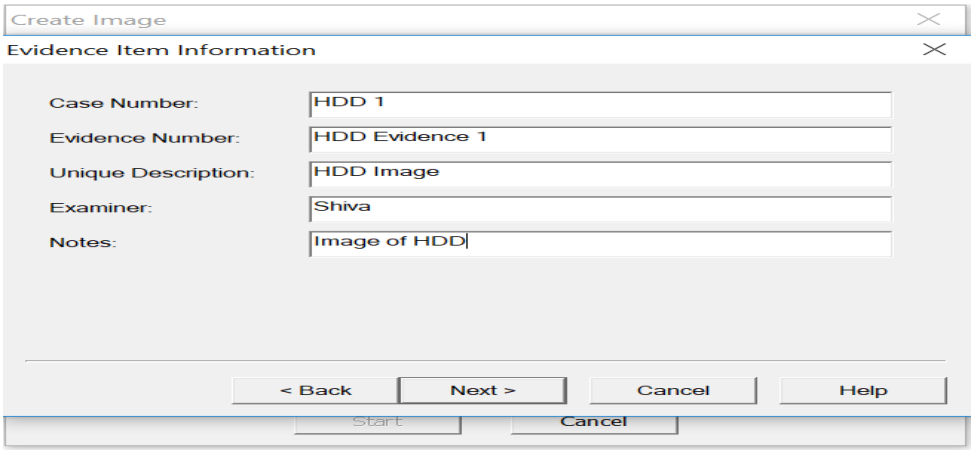

Figure 62. Assigning Name for Unique Identification of HDD Image

Image created of the drive is of the same size of the drive or greater than the size of the drive. If the image is greater than the size of the drive, then it would end up in failure if the size required for storing the image is insufficient. So, it is better to fragment the size of the image. In the image creation of HDD, the fragmentation size was set to 100GB. So, there will be 10 images in total for the disk image created.

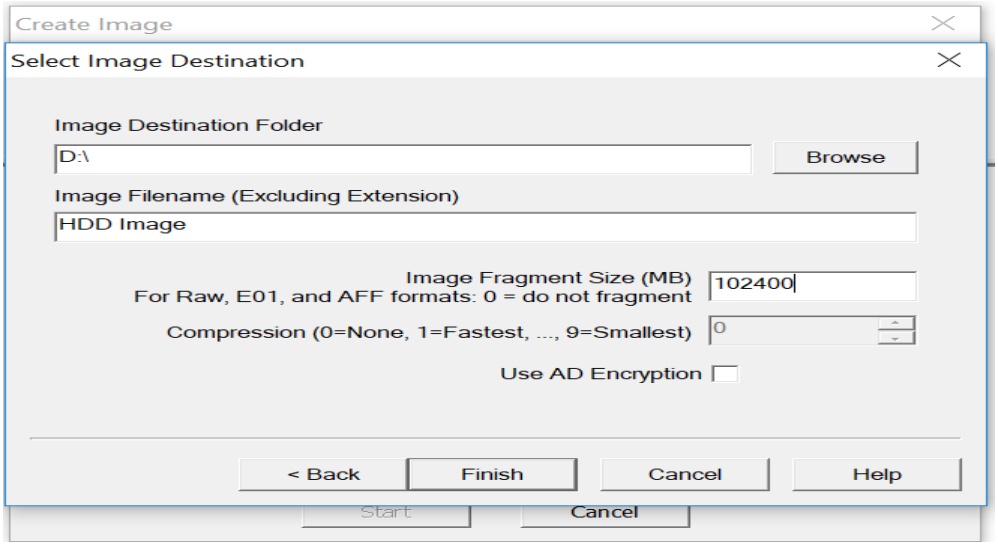

Figure 63. Selecting the Fragmentation Size for Image of HDD

As it is a large disk of 1TB, it is suggestible to check on pre-calculate progress statistics to estimate the time remaining for completion of the process.

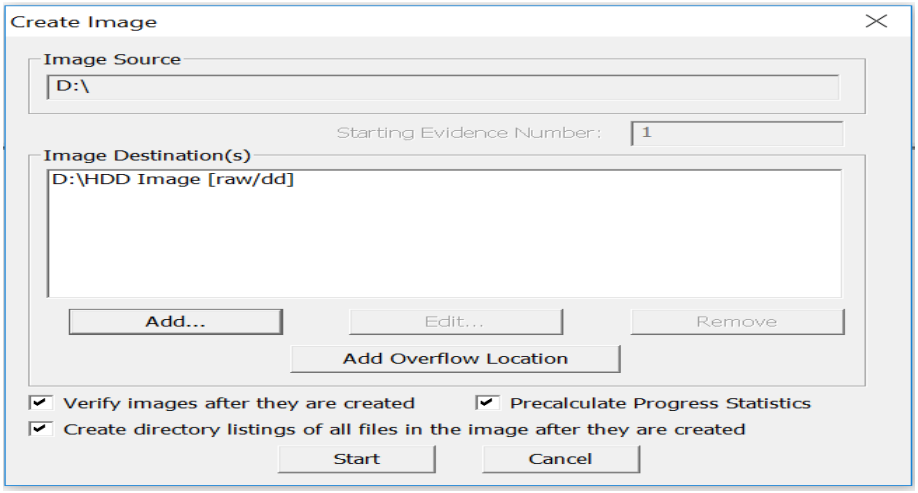

Figure 64. Verifying and Starting the Process of Image Creation of HDD

Random pictures were captured during different stages of the image creation of the HDD drive.

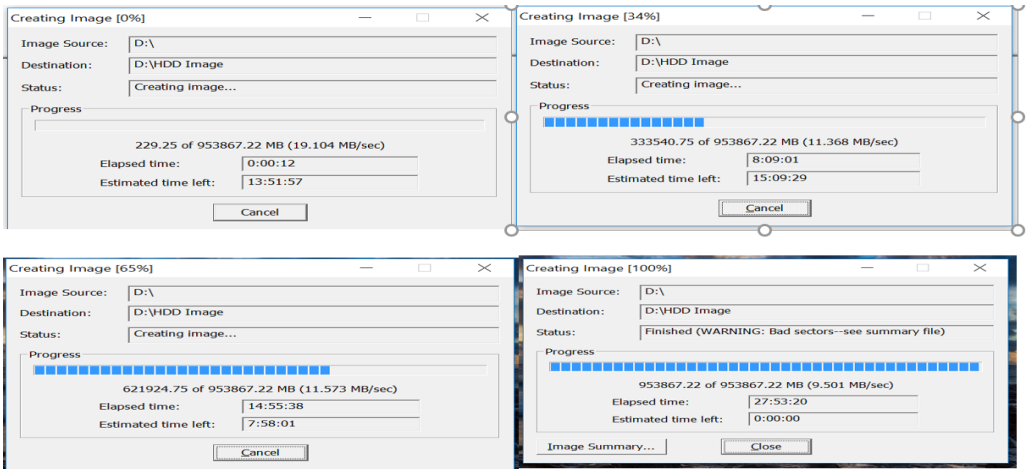

Figure 65. Image Creation of HDD at Different Intervals

It took 28 hours for creating a disk image of 1TB HDD. The following figures represent the image summary for the HDD Image.

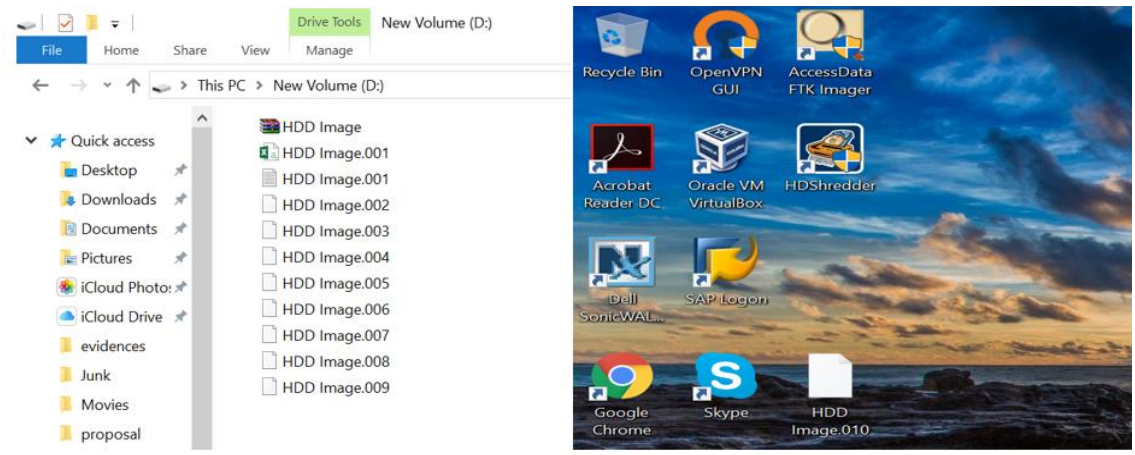

Figure 66. Image Created of HDD

Creating Image of SSD

The same process is followed in creating an image of SSD. Following are the screen shots captured for the same.

Figure 67. SSD Connected to Laptop 2

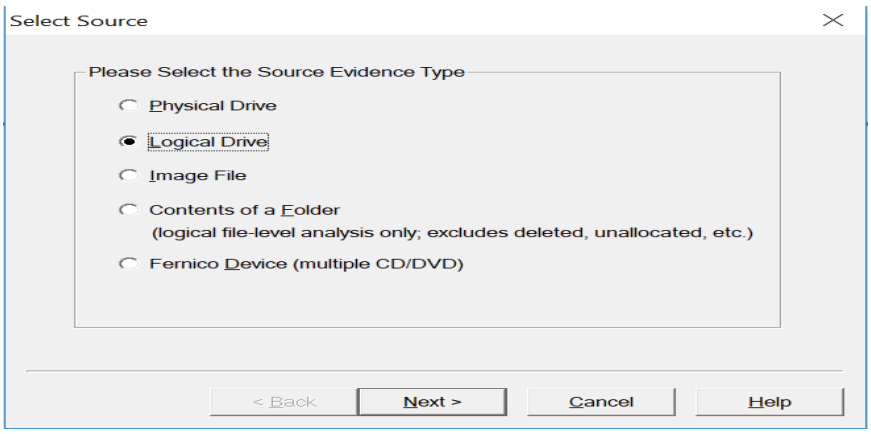

Figure 68. Selecting the Logical Drive for SSD Image Creation

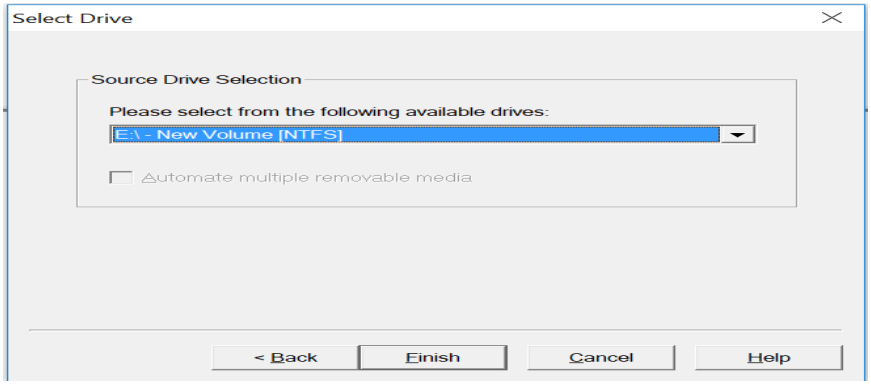

Figure 69. Selecting SSD Drive for Image Creation

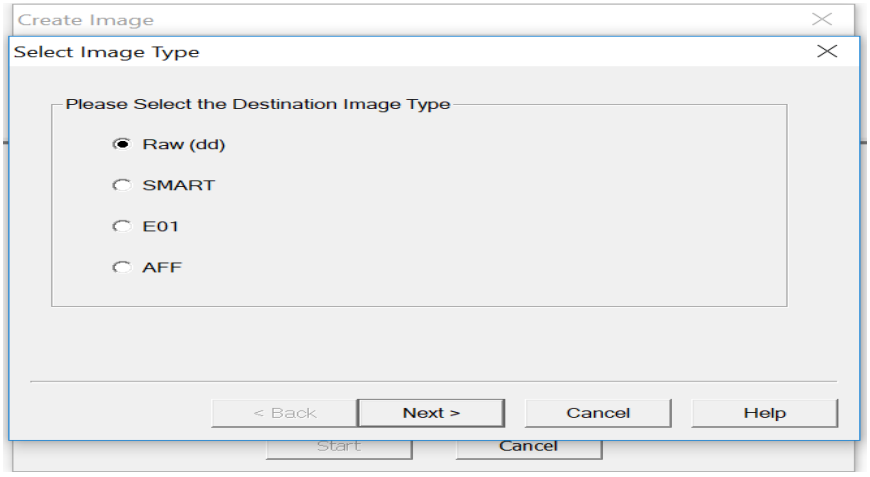

Figure 70. Selecting the Destination for Image of SSD

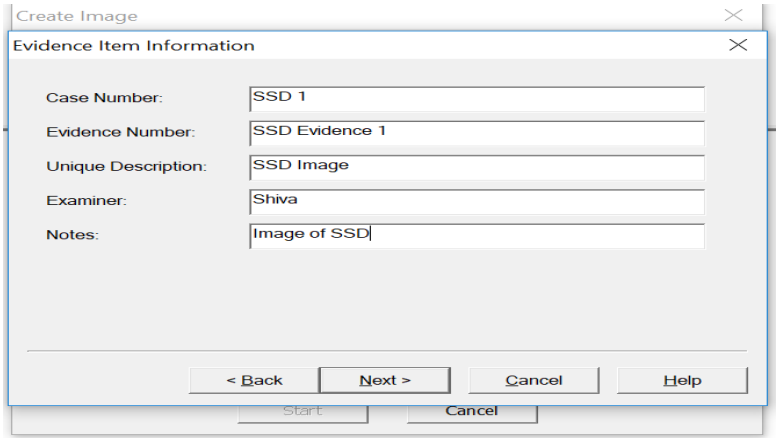

Figure 71. Selecting the Type of SSD Image

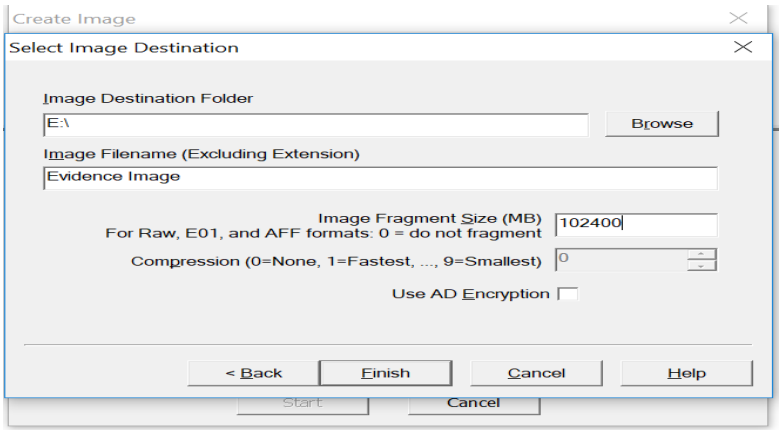

Figure 72. Selecting the Fragmentation Size for Image of SSD

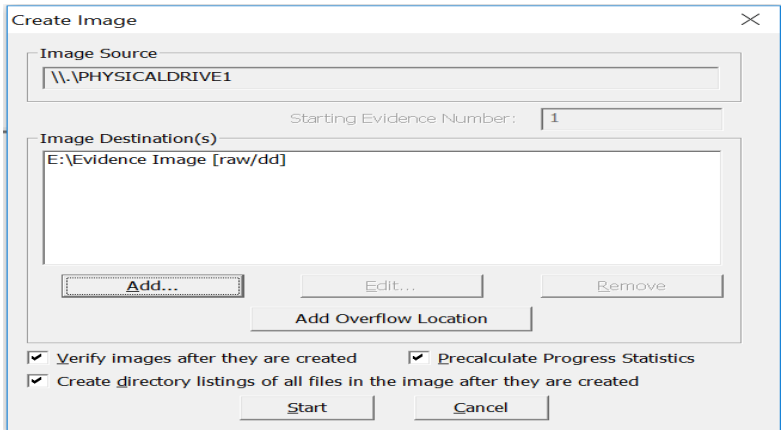

Figure 73. Verifying and Starting the Process of Image Creation of SSD

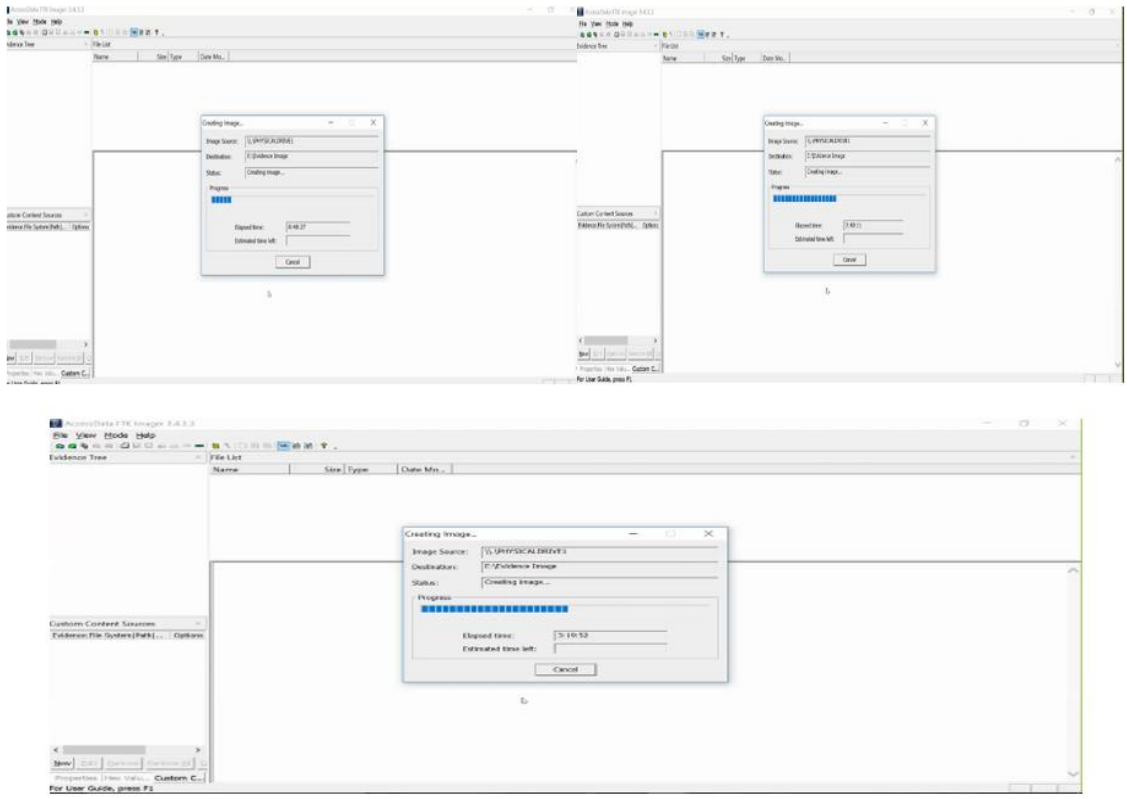

Figure 74. Image Creation of SSD at Different Intervals

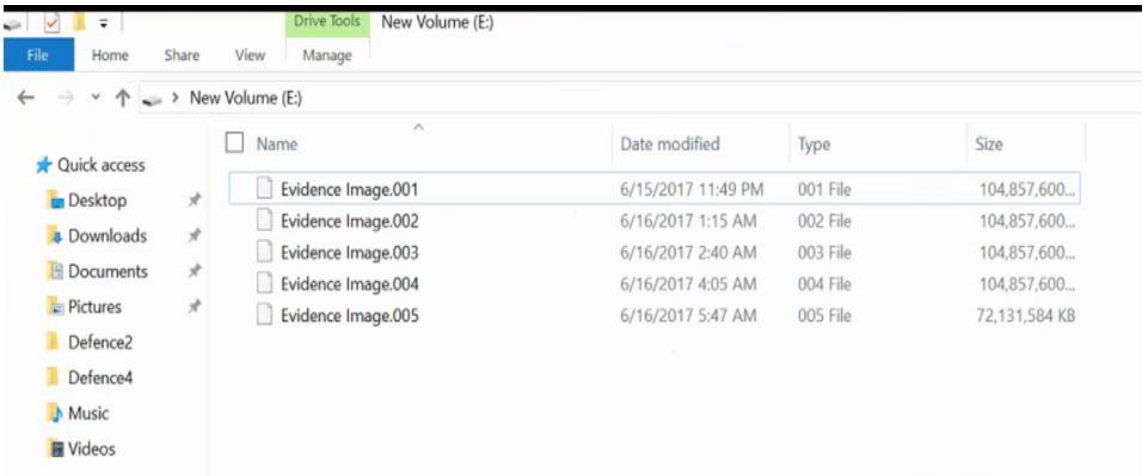

Figure 75. Images Created of SSD

Analyzing Image of HDD

Once the image file is created, it is analyzed using the investigator's laptop. The results obtained by the search of key words car, dose, islands, farmhouse, and mortgage are used for analyzing the functioning of evidence destruction in both HDD and SSD.

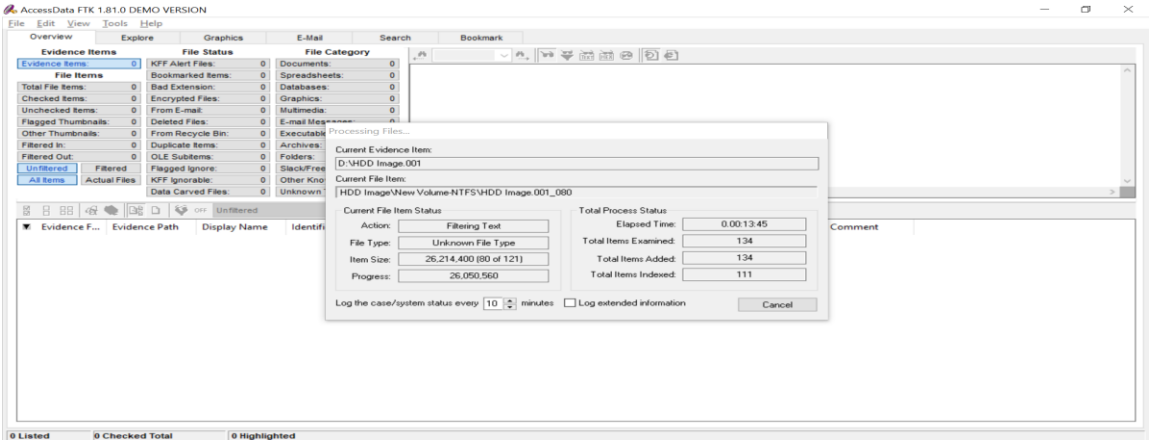

Figure 76. Processing Image 1 of HDD

After the completion of processing, a window appears where we can search for keywords or search each file one by one.

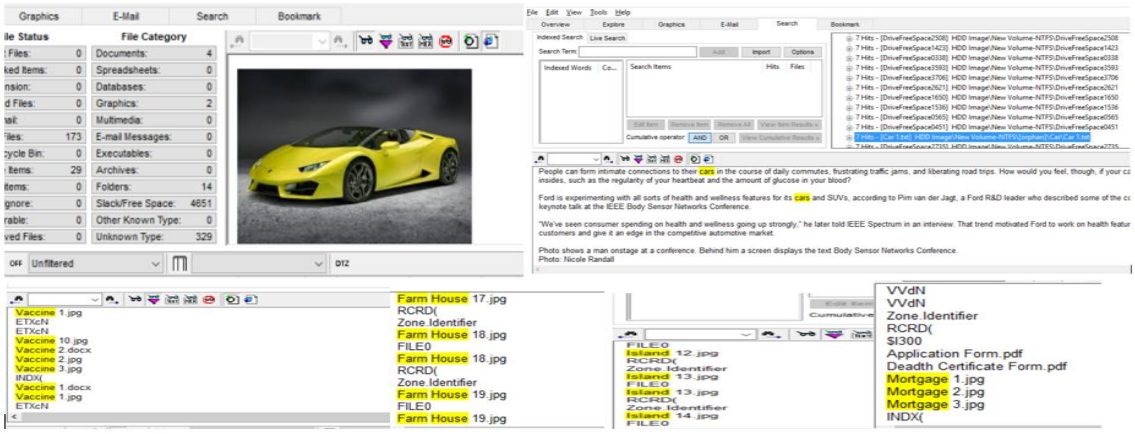

Figure 77. Files Identified by Searching Keywords in Image 1 of HDD

We will analyze the results by identifying the number of files and number of hits by individual keyword. Following are the results identified in Image 1 of HDD.

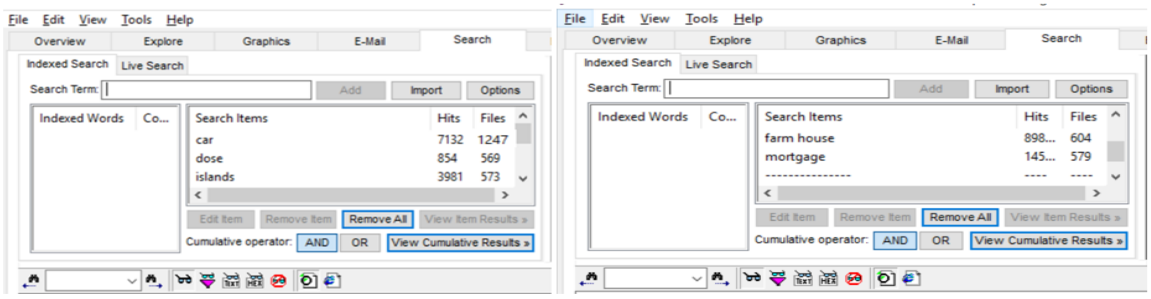

Figure 78. Results Identified in Image 1 of HDD

The same process is repeated for all other images that were created earlier which are as shown below.

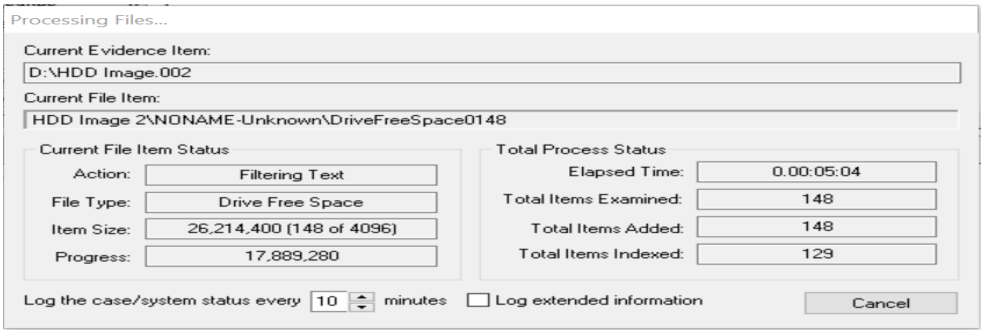

Figure 79. Processing Image 2 of HDD

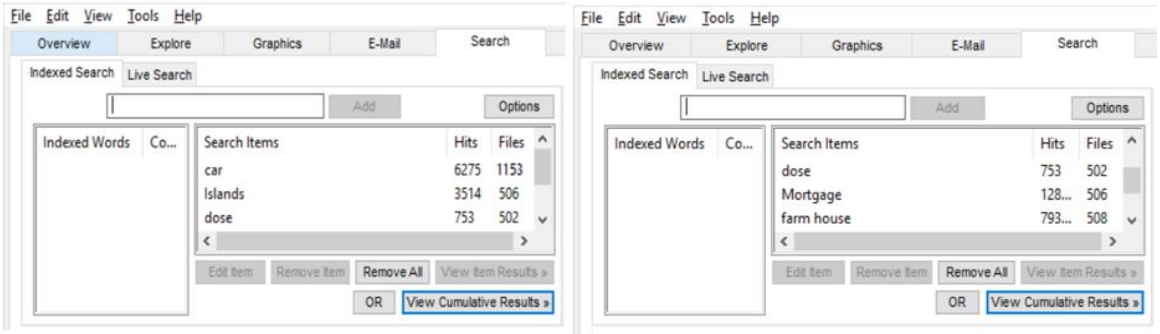

Figure 80. Results Identified in Image 2 of HDD

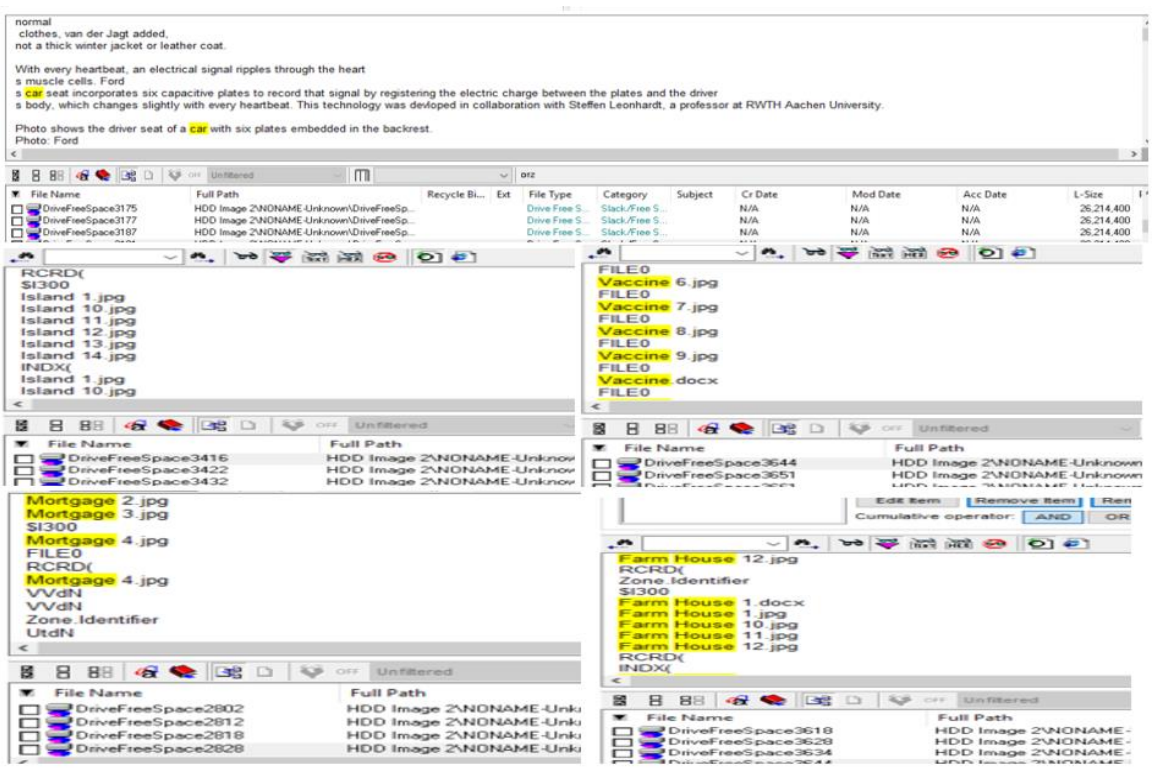

Figure 81. Files Identified by Searching Keywords in Image 2 of HDD

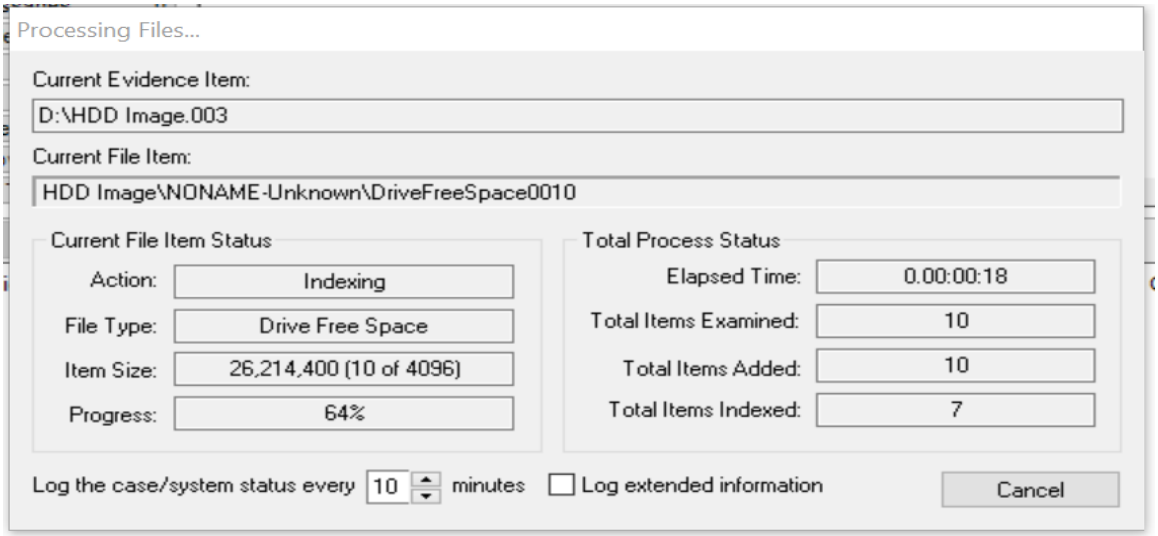

Figure 82. Processing Image 3 of HDD

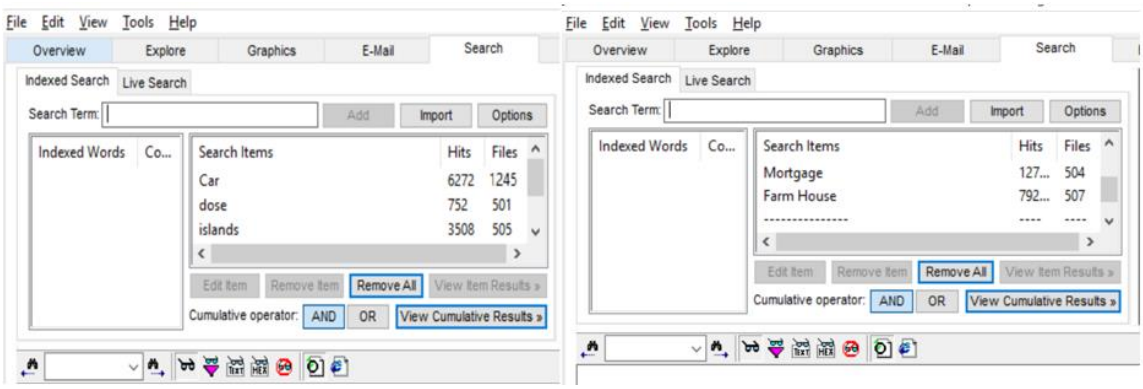

Figure 83. Results Identified in Image 3 of HDD

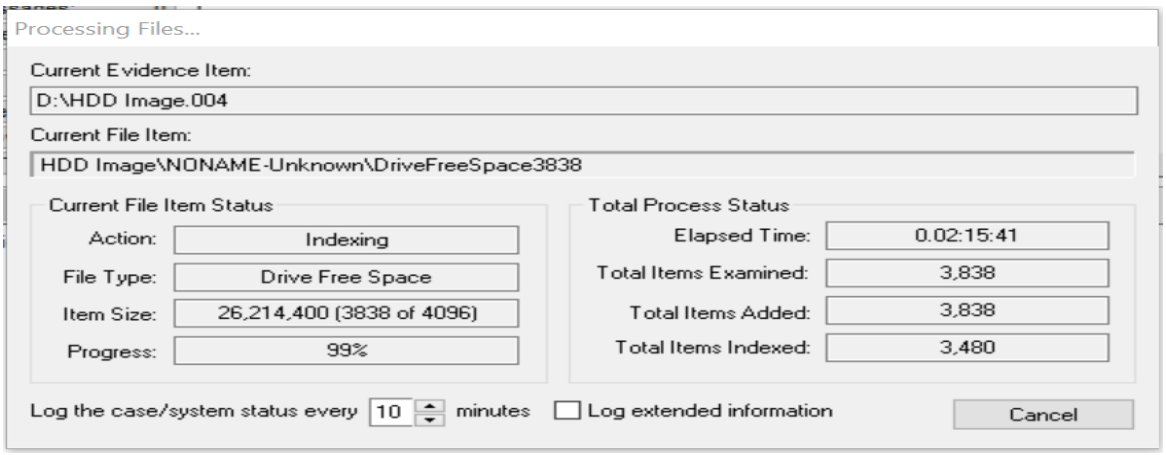

Figure 84. Processing Image 4 of HDD

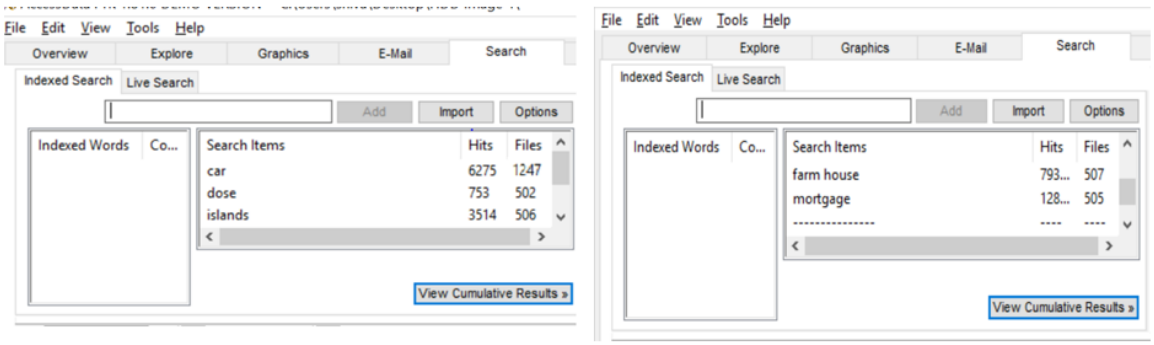

Figure 85. Results Identified in Image 4 of HDD

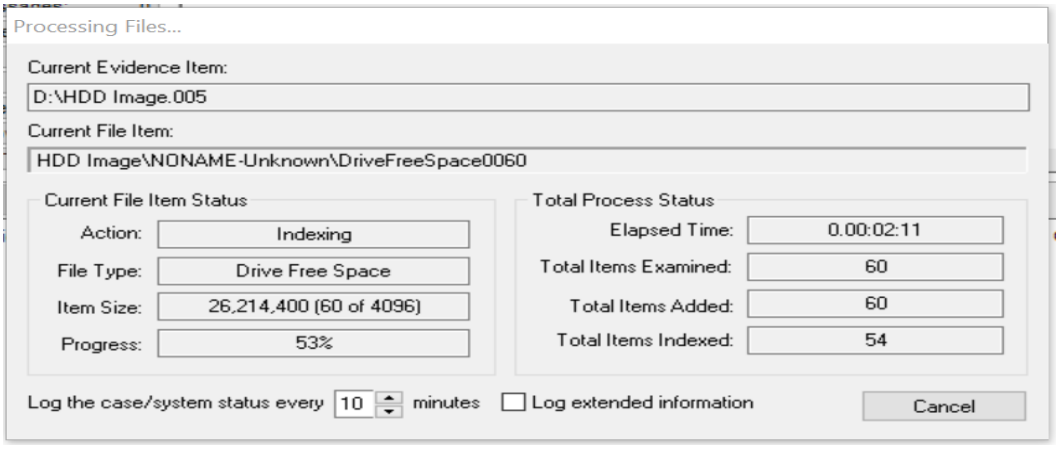

Figure 86. Processing Image 5 of HDD

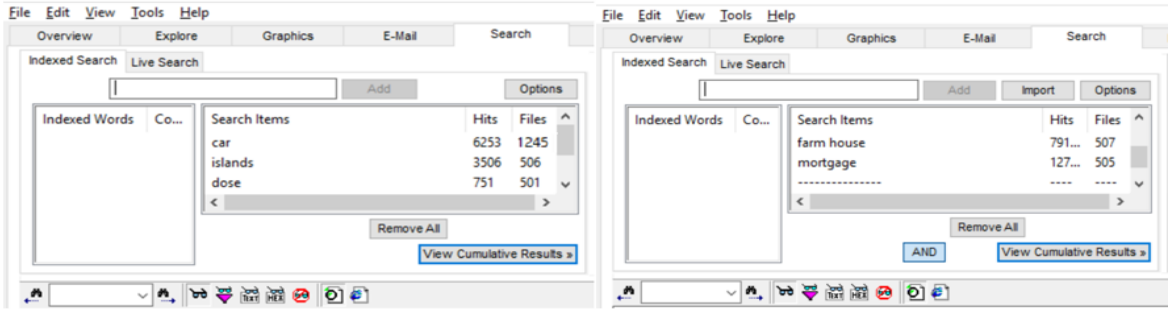

Figure 87. Results Identified in Image 5 of HDD

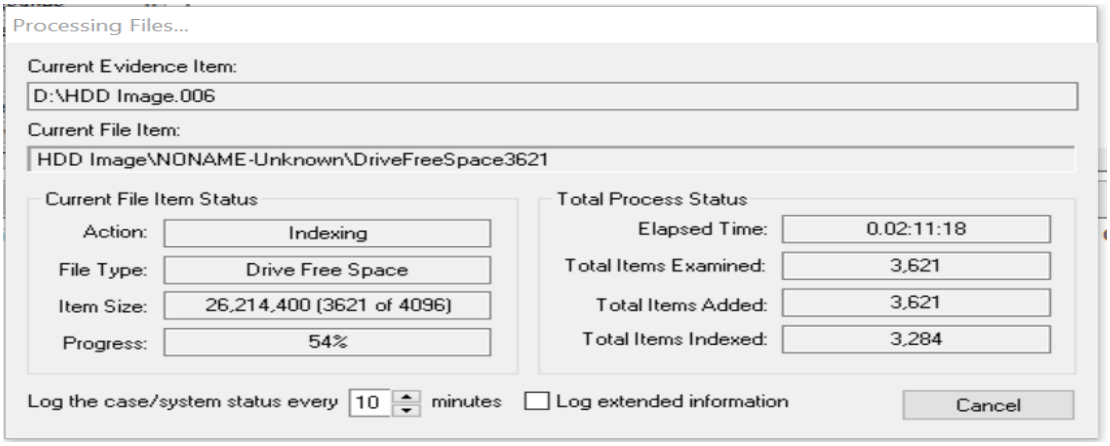

Figure 88. Processing Image 6 of HDD

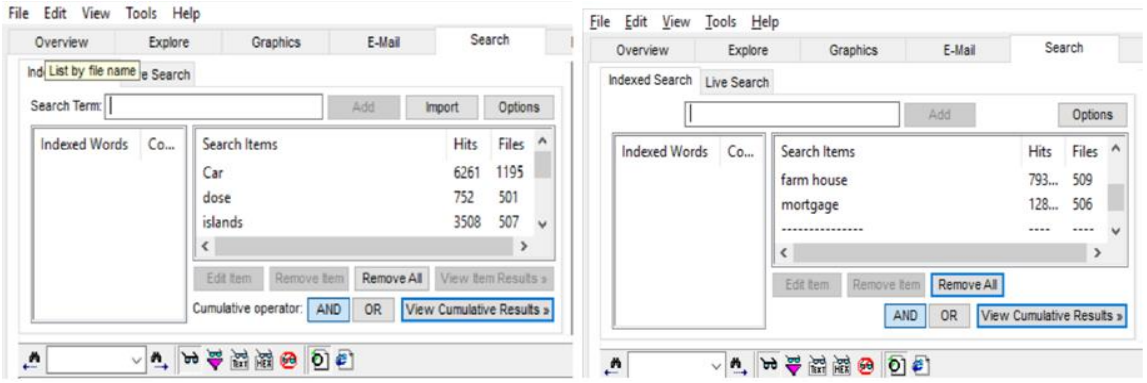

Figure 89. Results Identified in Image 6 of HDD

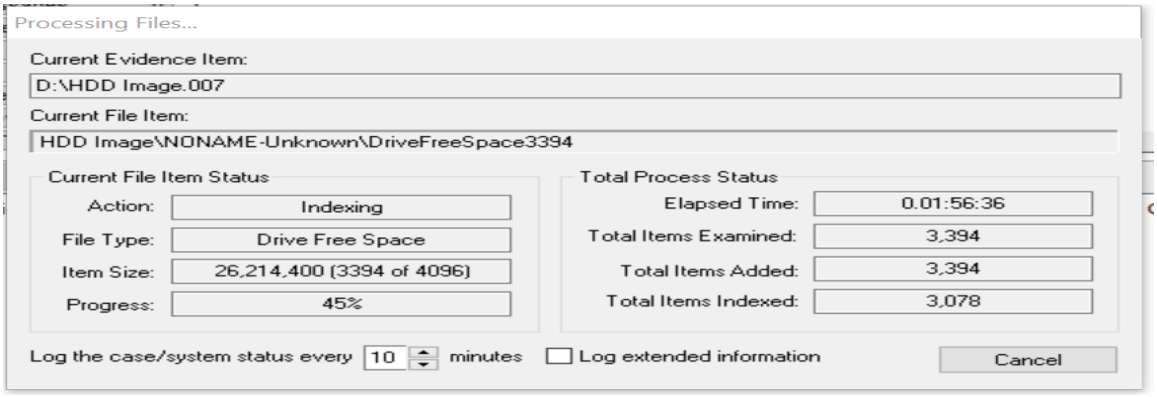

Figure 90. Processing Image 7 of HDD

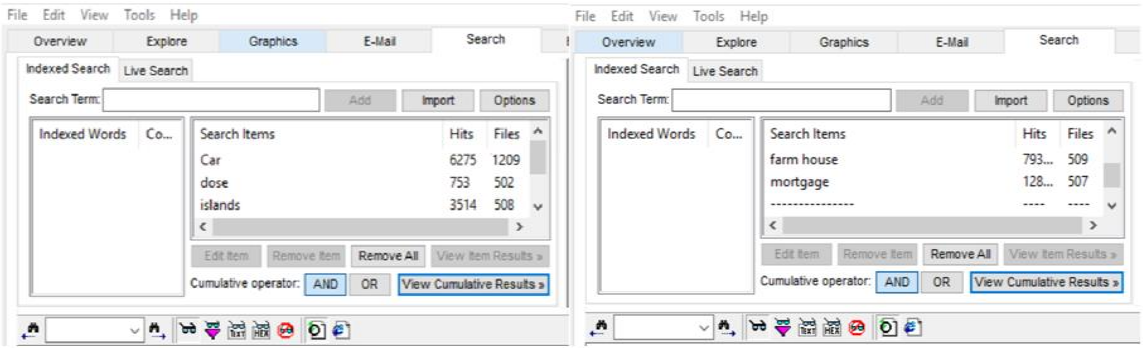

Figure 91. Results Identified in Image 7 of HDD

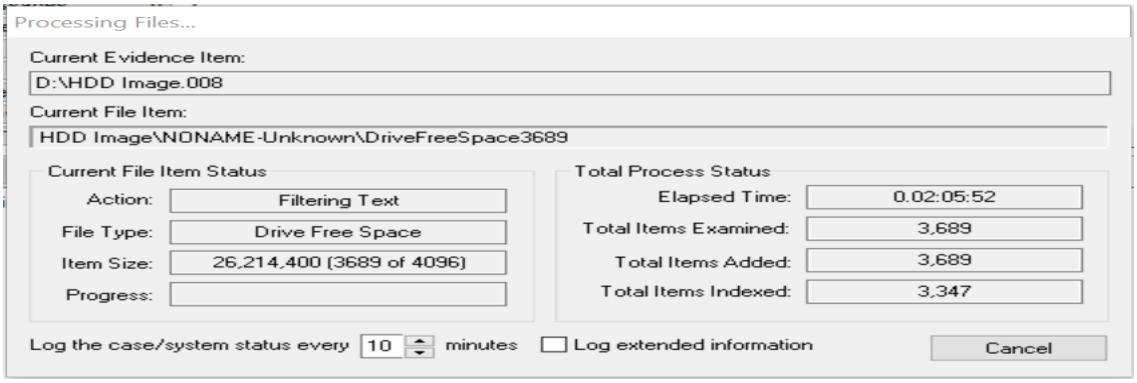

Figure 92. Processing Image 8 of HDD

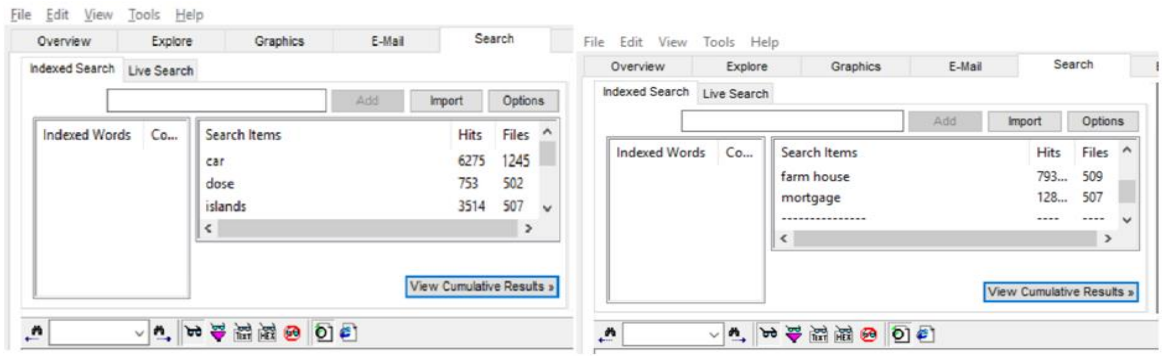

Figure 93. Results Identified in Image 8 of HDD

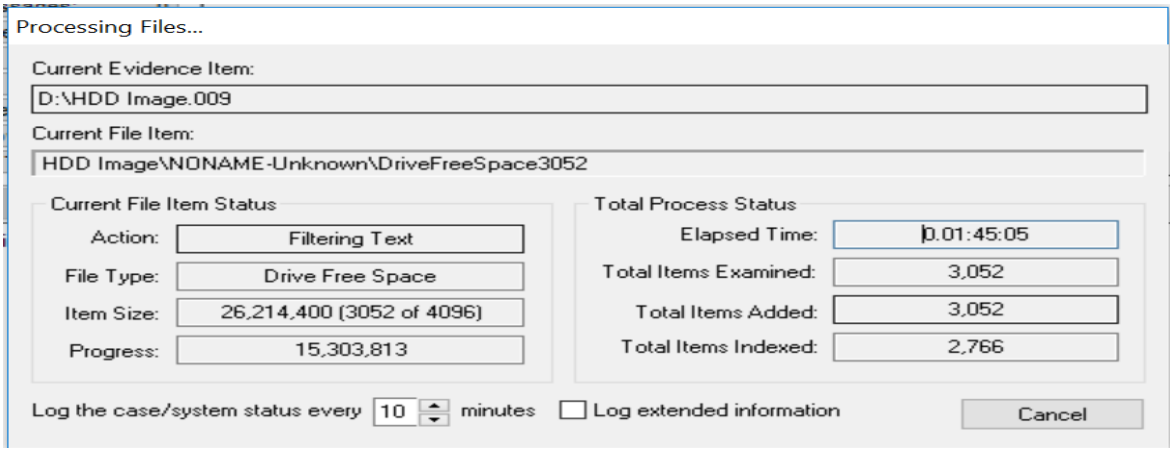

Figure 94. Processing Image 9 of HDD

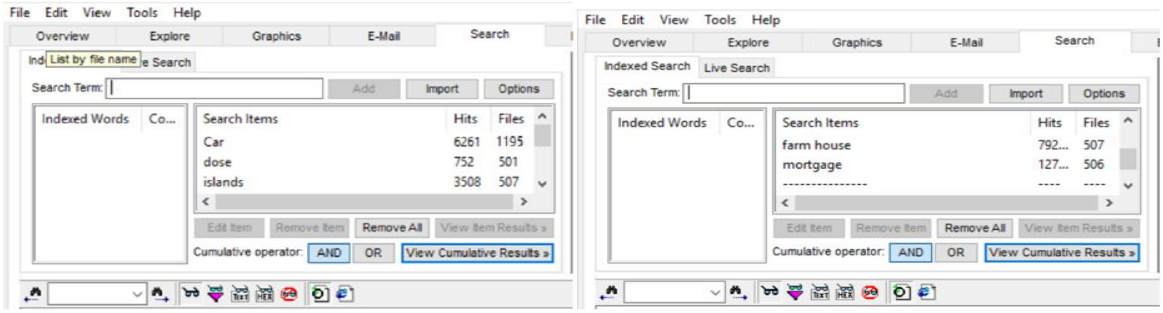

Figure 95. Results Identified in Image 9 of HDD

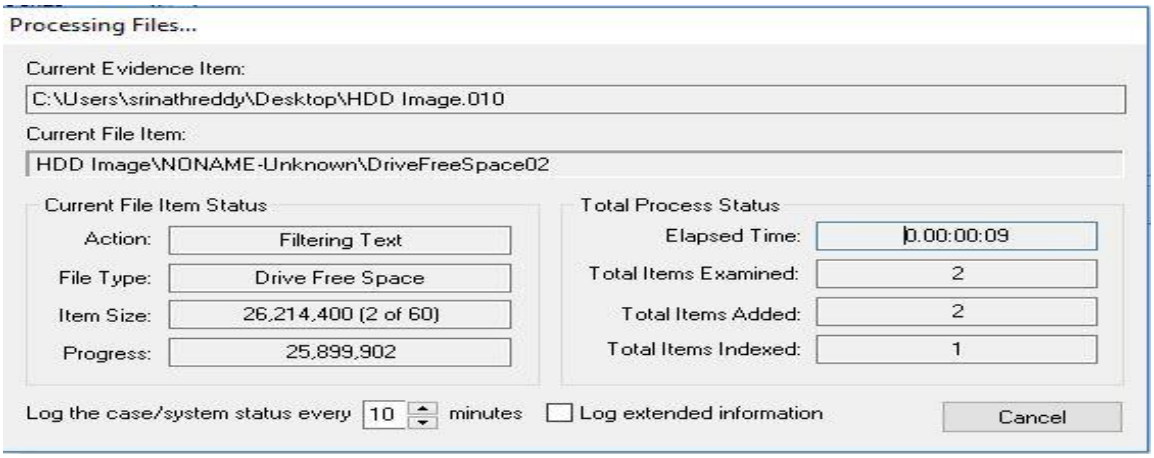

Figure 96. Processing Image 10 of HDD

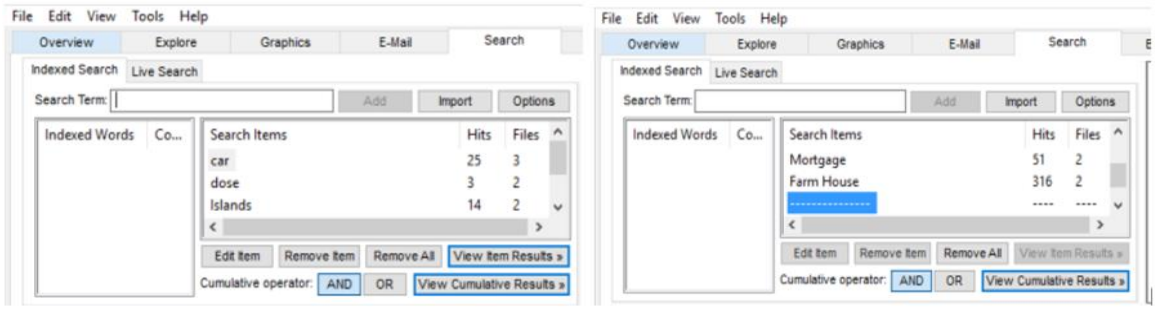

Figure 97. Results Identified in Image 10 of HDD

After analyzing the results of all the 10 images, an average of the hits and files identified in all 10 images is taken and is used for comparison with that of SSD.

Table 2

Results Obtained from Images of HDD

Keyword	Files in HDD	Hits in HDD
Car	1099	5731
Dose	460	688
Islands	462	3208
Farm House	467	7272
Mortgage	463	1201

Analyzing Image of SSD

The same process of Image creation and analyzing the images using FTK Toolkit is followed for SSD. Following are the steps followed.

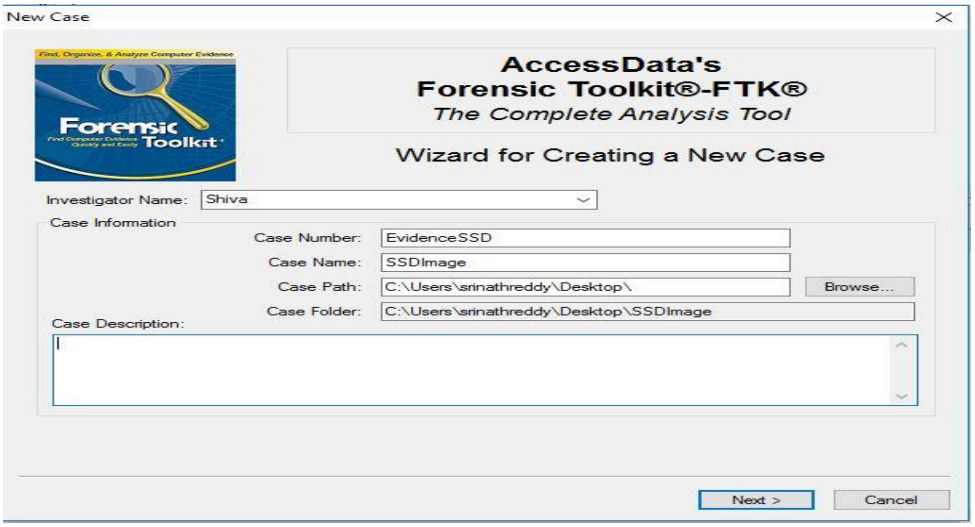

Figure 98. Assigning Case Name to Analyze the Image of SSD

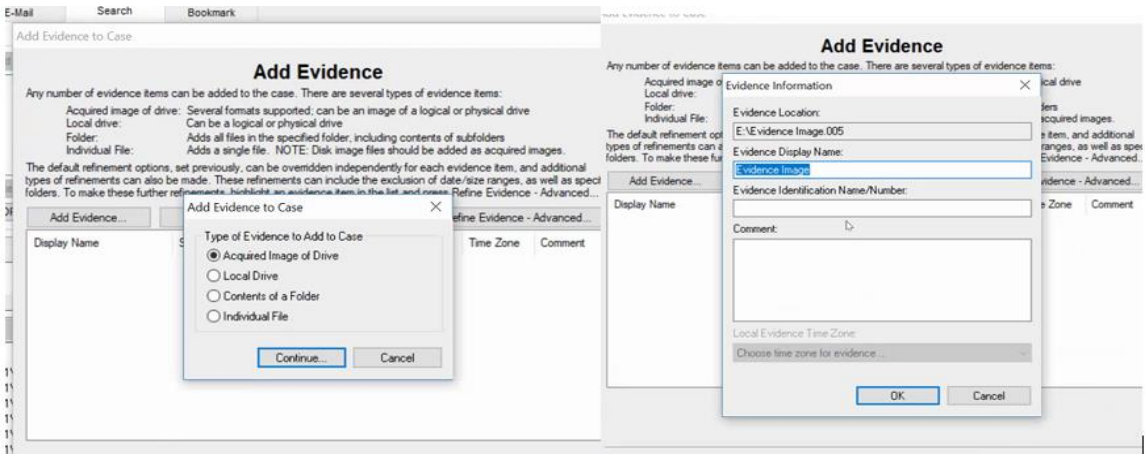

Figure 99. Adding Evidence to Analyze Results of SSD

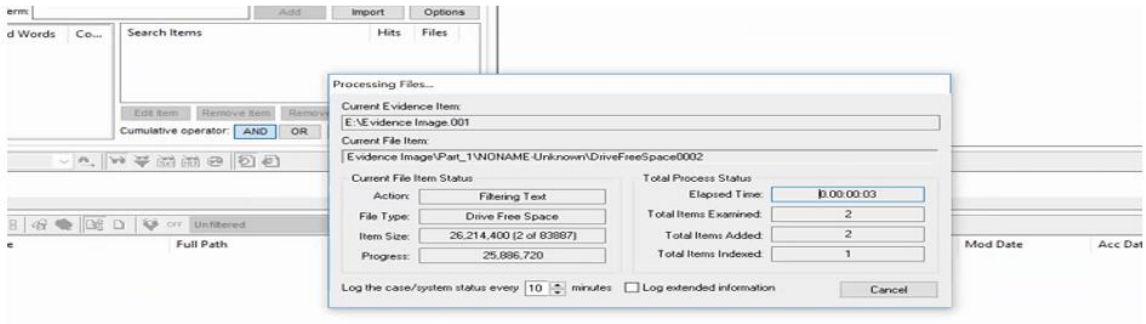

Figure 100. Processing Image 1 of SSD

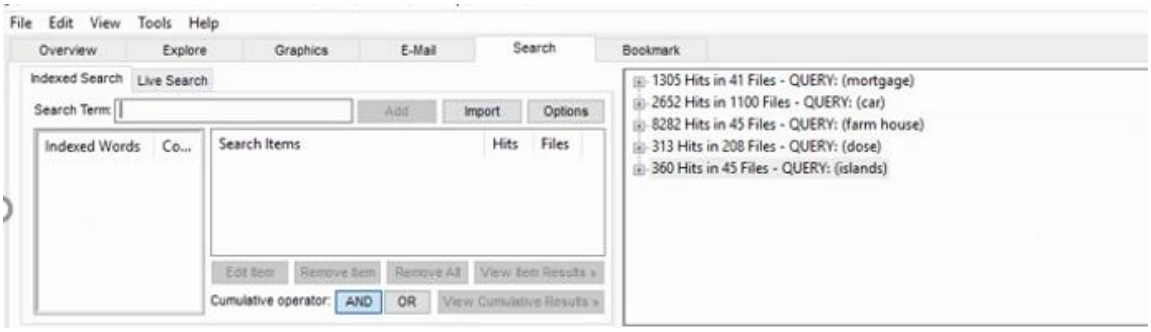

Figure 101. Results Identified in Image 1 of SSD

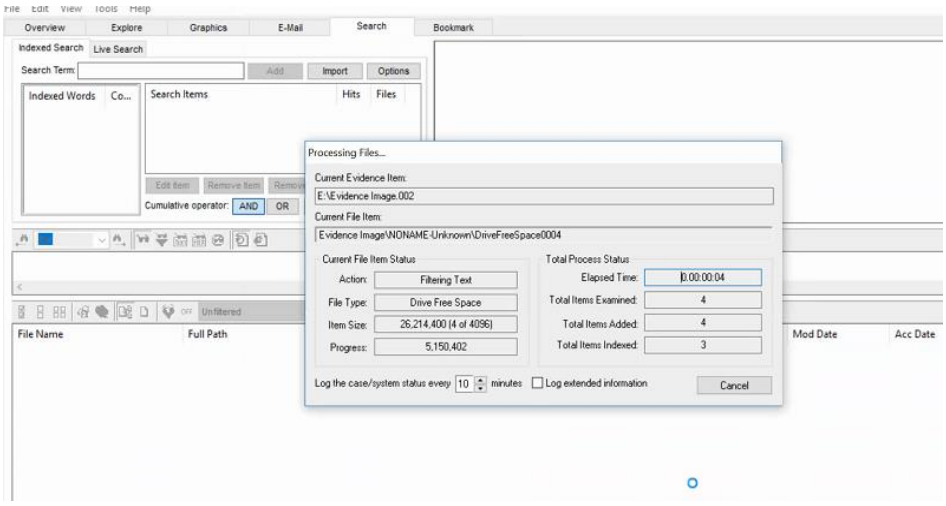

Figure 102. Processing Image 2 of SSD

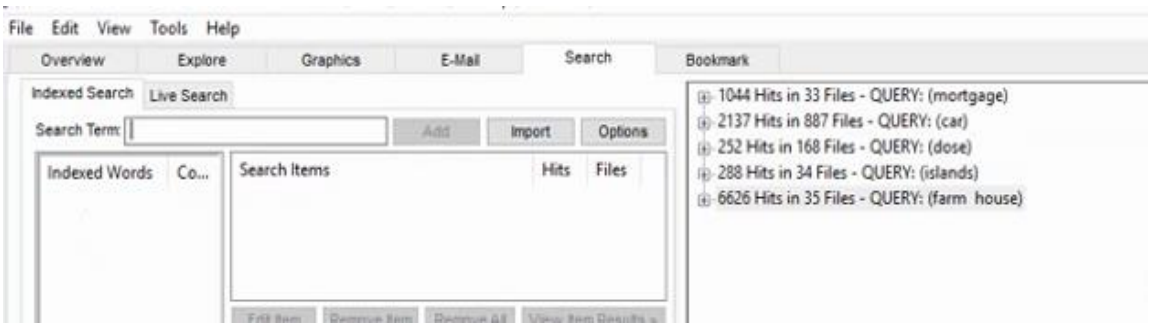

Figure 103. Results Identified in Image 2 of SSD

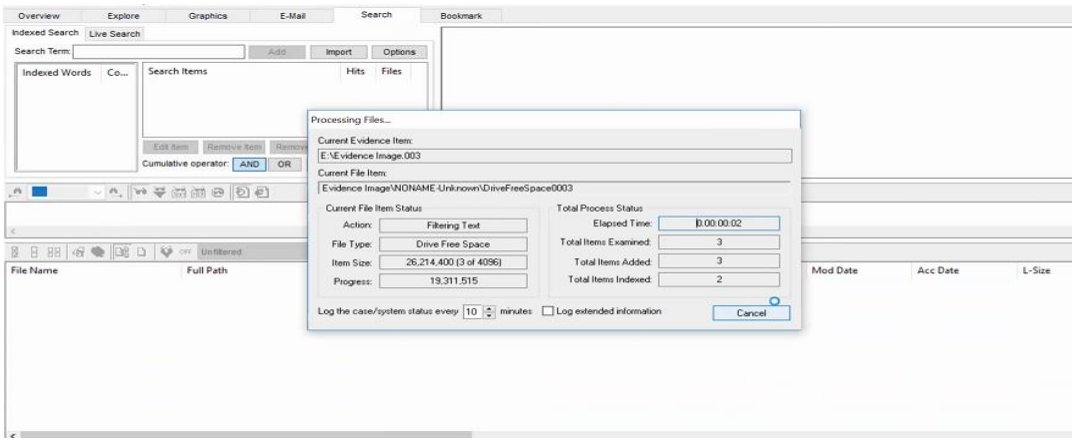

Figure 104. Processing Image 3 of SSD

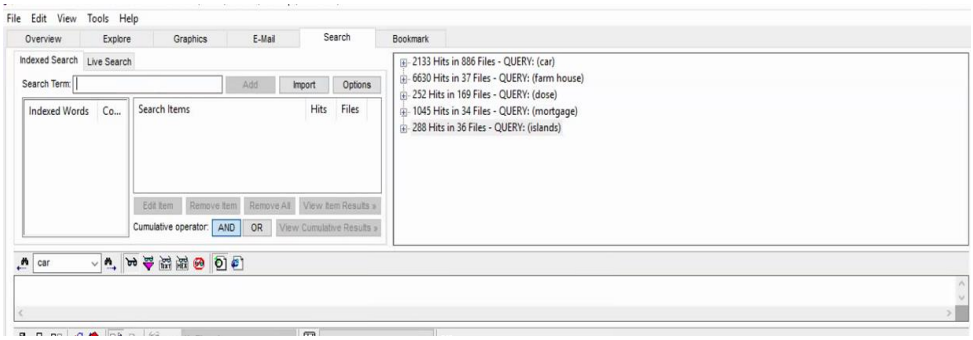

Figure 105. Results Identified in Image 3 of SSD

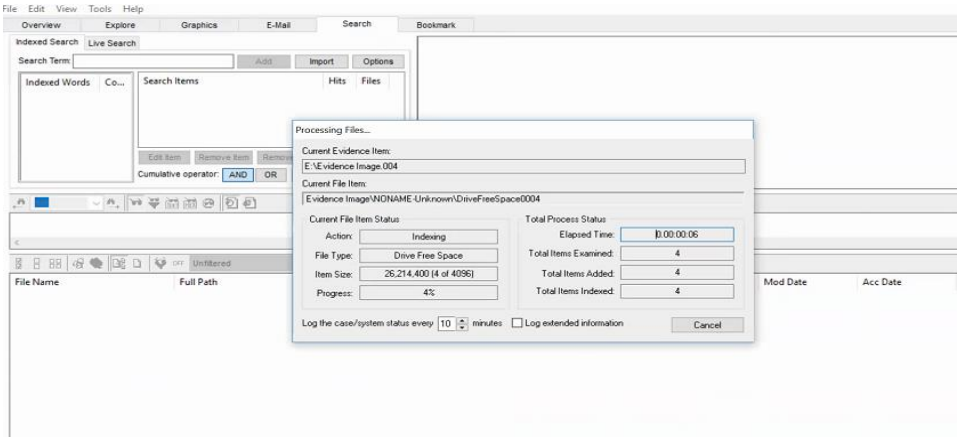

Figure 106. Processing Image 4 of SSD

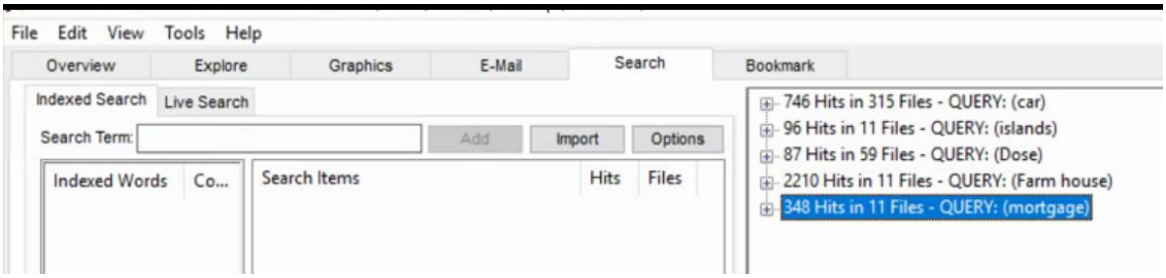

Figure 107. Results Identified in Image 4 of SSD

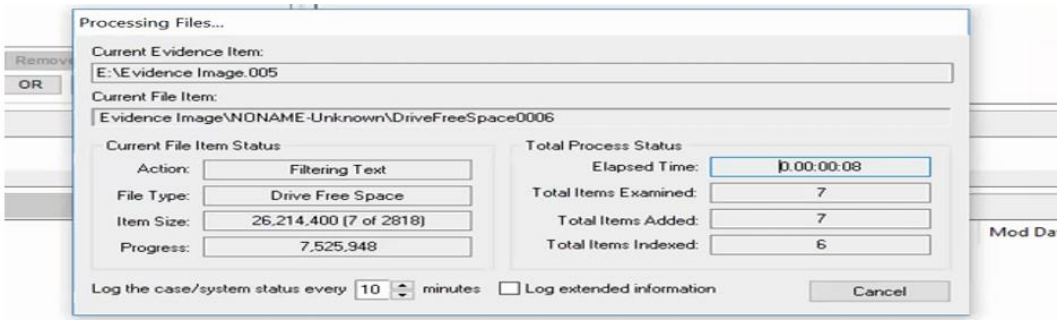

Figure 108. Processing Image 5 of SSD

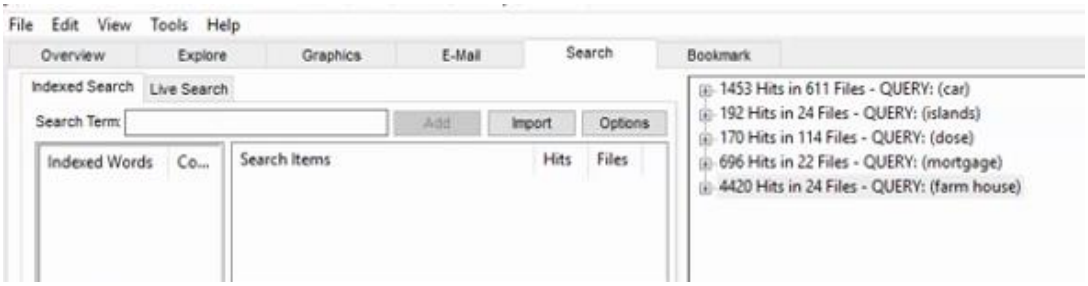

Figure 109. Results Identified in Image 5 of SSD

After analyzing the results of all the five images an average of the hits and files identified in all five images is taken and results are all follows.

Table 3

Results Obtained from Images of SSD

Keyword	Files in SSD	Hits in SSD
Car	760	1824
Dose	144	215
Islands	30	245
Farm House	31	5633
Mortgage	28	882

This table gives you an idea of the number of files that were identified by the key word searches. The word Car had 760 files in SSD as identified by the FTK Toolkit and it was

recognized for 1824 times in different files identified. Similarly, the key word farm house had 31 files as identified by FTK and was recognized for 5633 times in all different folders identified.

An image was created to analyze the original files and hits without any deletion or format process. This image included all the different combinations of files that were used in both the drives, but the combinations were not deleted every time but were kept in the folder to make sure we have an exact number of files and hits of the key words which we used in the experiment. The following figure shows the number of files and hits identified for the key word searches in the image of the folder which included all different combinations sent to both the drives.

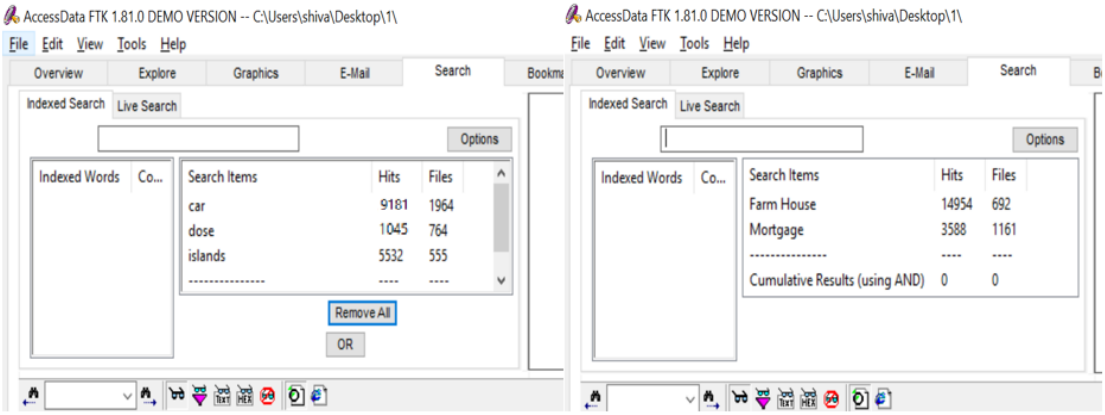

Figure 110. Results Identified in the Image of Different Combinations Used

We have the different results which were found by the key word searches in SSD, HDD and the original files and hits that were to be identified in both the drives. To make the comparison to be clear we will be using a tabular format as well as a pivot chart representation of all the results obtained. The following table compares the original number of files, hits with those identified in both HDD and SSD.

Table 4

Comparing the Results Obtained

Keyword	Original Files	Files in HDD	Files in SSD	Original Hits	Hits in HDD	Hits in SSD
Car	1964	1099	760	9181	5732	1824
Dose	764	460	144	1045	688	215
Islands	555	462	30	5532	3209	245
Farm House	692	467	31	14954	7202	5633
Mortgage	1161	463	28	3588	1201	882

It was found that the key word Car had 1964 files initially with all the different combinations of evidence folder, evidence trasher folders made and the word car was recognized for 9181 times in all the documents such as images, contents of word documents, excel sheets and note pads that were passed. However, we could find 1099 files out of 1964 files in HDD using FTK Toolkit. So, there were some key evidence files that were missing but it is a pretty good sign that even after formatting the disk after every combination made the FTK toolkit could identify 60% of the files that were deleted. But, this was not the case with SSD, we could only identify 760 files out of 1964 original files in SSD which is less than 40 percent of the original files. It's very difficult for the forensic investigator in this scenario for finding the suspect in a case when we were not able to identify even 50% of the key evidence.

Like the files comparison, the word Car was identified for 9181 times in all different folders, files, word documents, excel sheets, note pad etc. in the original image. We could identify 5732 times in that of an HDD which lands up at 65& of the key word being identified and it is a good sign for the investigator. However, 1824 times the key word was identified in SSD which is less than 20% of the original key word identified. This possesses

risk for the investigators in identify the key evidence and proving who the suspect is due to the key features of the SSD.

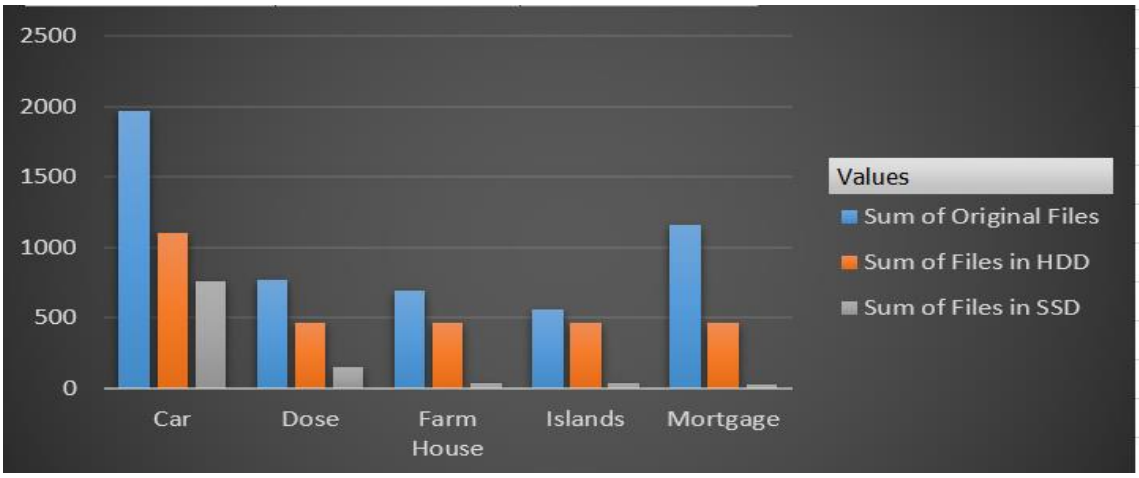

Figure 111. Difference in Results Identified by Number of Files

The graphical representation shown above is the comparison of the number of files that were being identified in the original image with that of identified in HDD and SSD. Considering the key word search of Farm House, it shows the number of files identified in an HDD is about 70-80% of the original files but when compared to that of an SSD we could see there were not even 10% of the files that were in the original folder. We can also notice that there is a vast difference in the number of files identified by an SSD in all the key word searches such as islands, mortgage, dose, and car.

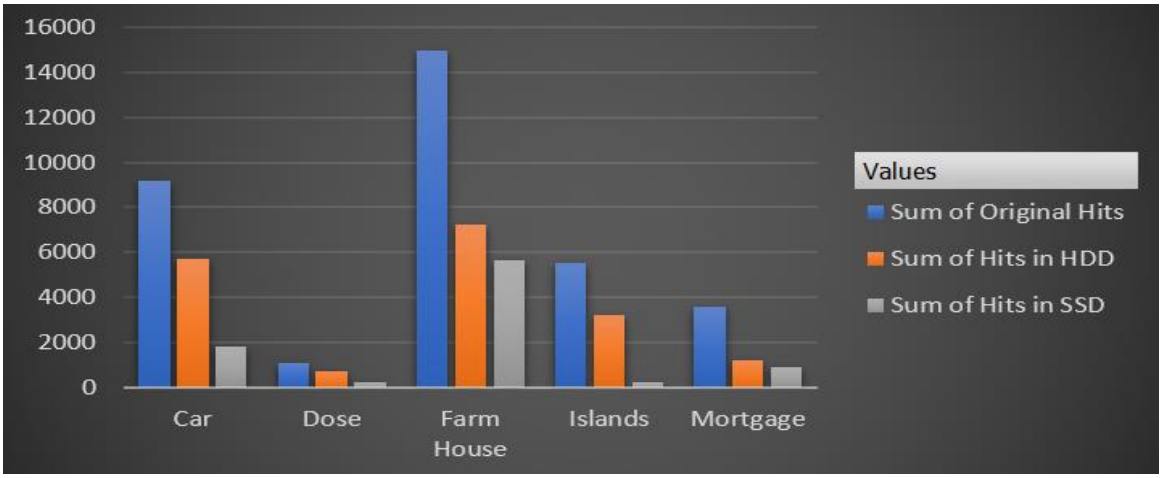

Figure 110. Difference in Results Identified by Number of Hits

The graphical representation shown above is the comparison of the number of hits that were being identified in the original image with that of identified in HDD and SSD. Considering the key word search of Islands, it shows the number of hits identified in an HDD is about 60% of the original files but when compared to that of an SSD we could see there were not even 10% of the hits that were in the original folder. The special features in SSD such as wear leveling, garbage collection, self-corrosion, TRIM command help SSD in destructing the key evidence on its own without any instructions from the computer. The results identified clearly give us a good conclusion on how forensic investigators are struggling with SSD.

Conclusion

Both the drives HDD and SSD are passed with the same evidence files, formatted at same intervals, and passed with random data and different combination of evidence destruction files are being transferred. Images of the drives are being created using FTK Imager and are carefully being analyzed in the investigator's laptop using FTK Toolkit. However, it is clearly noticeable that even after performing the same set of operations on both the drives the results obtained do not match.

We have discussed the key features that Solid-state drives hold such as wear leveling, TRIM, Garbage collection which helps to destroy the evidence in SSD on its own. Based on this experiment and the results obtained it is proven that SSD's possess evidence destruction phenomenon that creates trouble for the forensic investigators for finding key evidence and resolving cases that were solved by using traditional methods on HDD.

Future Work

It is proven by the help of this experiment that formal traditional methods used on HDD's by forensic investigators for solving the key cases do not hold good in case of solid-state drives. Forensic investigators need to come up with new methods to overcome the destruction capacity of the solid-state drives. As researchers stated that solid-state drives are beginning the end of current practice in digital forensic recovery, it is the time for forensic investigators to review the current techniques used and emerge with new tools for cracking even the self-destructed files in Solid-state drives. If new techniques are not being introduced, it would result in the rise of crimes which do not have evidence to be proven and give chance for crime committers to consider these loop holes and increase the crime rate.

References

Aaronson, L. (2008). *How it works: The sturdiest solid-state storage*. Retrieved from http://www.popsci.com/node/19967 dated 04-15-2017.

Ashcroft, J. (2001). *Electronic crime scene investigation: A guide for first responders*. Washington. DC: U.S. Department of Justice, Retrieved from https://www.ncjrs.gov/pdffiles1/nij/187736.pdf dated 04-15-2017.

Bajorek, C. H. (2014). *Magnetoresistive (MR) heads and the earliest mr head-based disk drives: Sawmill and corsair*. Retrieved from http://s3.computerhistory.org/groups/magnetoresistive-heads.pdf dated 04-15-2017.

Baxter, A. (2015). *SSD vs HDD*. Retrieved from Storageeview.com Retrieved from http://www.storagereview.com/ssd_vs_hdd dated 04-15-2017

Belkasoft. (2014). *Recovering evidence from SSD Drives in 2014: Understanding TRIM, garbage collection and exclusions*. Retrieved from Forensic Focus retrieved from http://articles.forensicfocus.com/2014/09/23/recovering-evidence-from-ssd-drives-in-2014-understanding-trim-garbage-collection-and-exclusions/ dated 04-15-2017.

Bell, G. B. (2010). Solid state drives: The beginning of the end for current practice in digital forensic recovery? *Journal of Digital Forensics, Security and Law*. Retrieved from http://ojs.jdfsl.org/index.php/jdfsl/article/viewFile/21/45 dated 04-15-2017.

Bodo, M. (1996). *Hard drive bible.* Sunnyvale, CA: Corporate Systems Center.

Brendan, H. (2017). *The battle between SSD and HDD is over, and the winner is clear*. Retrieved from Yahoo Tech: https://www.yahoo.com/tech/battle-between-ssd-hdd-over-141508916.html dated 04-15-2017

Cactus. (2014). *Wear levelling - static, dynamic and global*. Retrieved from Cactus Technologies Retrieved from https://www.cactus-tech.com/files/cactus-tech.com/documents/whitepapers/Wear%20Leveling%20-%20Static%20-%20Dynamic%20-%20Global.pdf dated 04-15-2017

Corsair. (2007). *USB flash wear-leveling and life span*. Retrieved from https://web.archive.org/web/20071013150729/http://www.corsair.com/_faq/FAQ_flash_drive_wear_leveling.pdf dated 04-15-2017.

Daniel, E. D. (2011). *Magnetic recording technology*. Columbus, OH: McGraw-Hill.

Devine, R. (2016). *SSD vs HDD: Which should I have in my PC?* Retrieved from Windows Central, Retrieved from http://www.windowscentral.com/ssd-vs-hdd-which-should-i-have-my-pc dated 04-15-2017

Digital forensics. (n.d.). *In Wikipe*dia. Retrieved from https://en.wikipedia.org/wiki/Digital_forensics

Domingo, J. S. (2015). *SSD vs. HDD: What's the difference*? Retrieved from http://www.pcmag.com/article2/0,2817,2404258,00.asp dated 04-15-2017.

Domingo, J. S. (2017). *SSD vs. HDD: What's the difference?* Retrieved from PC Reviews. Retrieved from http://www.pcmag.com/article2/0,2817,2404258,00.asp dated 04-15-2017

Eleftheriou, E. (2009). *Write amplification analysis in flash-based solid state drives*. Retrieved from http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.154.8668 dated 04-15-2017.

Evans, C. (2012). *Flash! All-solid-state arrays*. Retrieved from http://searchstorage.techtarget.com/magazineContent/Flash-All-solid-state-arrays dated 04-15-2017.

Goble, G. (2012). Solid state drives buying guide: SSD hard drives made simple. *Digital Trends*. Retrieved from http://www.digitaltrends.com/computing/solid-state-drives-buying-guide-ssd-hard-drives-made-simple/ dated 04-15-2017.

Gubanov, Y. (2012). *Why SSDs destroy cort evidence, and what can be done about it*. Retrieved from Belkasoft: https://belkasoft.com/en/why-ssd-destroy-court-evidence dated 04-15-2017.

Handy, J. (2012). *How controllers maximize SSD life: Better wear leveling*. Retrieved from http://thessdguy.com/how-controllers-maximize-ssd-life-better-wear-leveling/ dated 04-15-2017.

Hard disk drive. (n.d.). *In Wikipedia*. Retrieved from https://en.wikipedia.org/wiki/Hard_disk_drive Retrieved 04-15-2017. Page last updated 04-15-2017

Hesse, B. (2017). *The battle between SSD and HDD is over, and the winner is clear*. Retrieved from http://www.digitaltrends.com/computing/solid-state-drives-vs-hard-disk-drives/ dated 04-15-2017

Hutchinson, L. (2012). *Solid-state revolution: in-depth on how SSDs really work*. Retrieved from http://arstechnica.com/information-technology/2012/06/inside-the-ssd-revolution-how-solid-state-disks-really-work/ dated 04-15-2017.

Justice, N. I. (2007). Investigations involving the internet and computer networks. *U.S. Department of Justice*. Retrieved from https://www.ncjrs.gov/pdffiles1/nij/210798.pdf dated 04-15-2017.

Kipp, S. (2015). Will SSD replace HDD? *IEEE*. Retrieved from http://www.ieee802.org/3/CU4HDDSG/public/sep15/Kipp_CU4HDDsg_01a_0915.pdf dated 04-15-2017.

Lal, A. (2009). *The SSD anthology: Understanding SSDs and new drives from OCZ.* Retrieved from http://www.anandtech.com/print/2738 dated 04-15-2017.

Mamun, A. A., Guo, G., & Bi, C. (2007). *Hard disk drive: Mechatronics and control.* Boca Raton, FL: CRS Press.

Masuoka, F. (1987). New ultra high density EPROM and flash EEPROM with NAND structure cell. *IEEE*, Electron Devices Meeting, 1987 International. IEEE Retrieved 04-15-2017.

Memon, N. (2009). *Challenges of SSD forensic analysis*. Retrieved from http://digital-assembly.com/technology/research/talks/challenges-of-ssd-forensic-analysis.pdf dated 04-15-2017.

Mueller, S. (2015). *Upgrading and repairing PCs* . Indianapolis, IN: Que Publishing.

Ngo, D. (2012). *Storage talk: Why you should get an SSD and keep your HDD, too.* Retrieved from https://www.cnet.com/news/storage-talk-why-you-should-get-an-ssd-and-keep-your-hdd-too/ dated 04-15-2017.

Ngo., D. (2013). *Digital storage basics, Part 4: SSD explained*. Retrieved from CNet: https://www.cnet.com/how-to/digital-storage-basics-part-4-ssd-explained/ dated 04-15-2017

Schrödinger's cat. (n.d.). *In Wikepedia*. Retrieved from https://en.wikipedia.org/wiki/Schr%C3%B6dinger%27s_cat

Seagate. (2012). *The top 20 things to know about SSD.* Retrieved from Seagate. Retrieved from http://www.seagate.com/files/docs/pdf/ssd-faq-us.pdf dated 04-15-2017

Security, A. B. (2009). Digital forensic: An introduction. *American Board of Information Security and Computer Forensics*. Retrieved from http://www.abchs.com/xsecure/chs/coursedocs/SSI_R1/pdf/DigitalForensics.pdf dated 04-15-2017.

Service, U. S. (2009). *Best practices for seizing electronic evidence*. United States Secret Service. Retrieved from http://www.forwardedge2.com/pdf/bestPractices.pdf dated 04-15-2017.

Smith, K. (2011). *Understanding SSD Over-provisioning*. Retrieved from https://www.flashmemorysummit.com/English/Collaterals/Proceedings/2012/20120822_TE21_Smith.pdf dated 04-15-2017.

Solid-state drive. (n.d.). *In Wikipedia*. Retrieved from https://en.wikipedia.org/wiki/Solid-state_drive Retrieved 04-15-2017. Page last updated 04-15-2017

Solomon, M. B. (2005). *Computer forensics jumpstart*. San Francisco, CA: Sybex.

Tokar, L. (2012). *Garbage collection and TRIM in SSDs explained* . Retrieved from The SSD Review. Retrieved from http://www.thessdreview.com/daily-news/latest-buzz/garbage-collection-and-trim-in-ssds-explained-an-ssd-primer/2/ dated 04-15-2017

Wei, M. G. (2010). *Reliably erasing data from flash-based solid state drives*. Retrieved from http://www.usenix.org/events/fast11/tech/full_papers/Wei.pdf dated 04-15-2017.

Woodford, C. (2015). *Hard drives*. Retrieved from Explain That Stuff:

http://www.explainthatstuff.com/harddrive.html dated 04-15-2017