## St. Cloud State University theRepository at St. Cloud State

Culminating Projects in Information Assurance

Department of Information Systems

5-2019

# Analysis of The Typical Performance Routines for Recovering Data from Solid State Drive During a Forensic Acquisition

Bhargav Rajammagari brajammagari@stcloudstate.edu

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

#### **Recommended** Citation

Rajammagari, Bhargav, "Analysis of The Typical Performance Routines for Recovering Data from Solid State Drive During a Forensic Acquisition" (2019). *Culminating Projects in Information Assurance*. 85. https://repository.stcloudstate.edu/msia\_etds/85

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

## Analysis of the Typical Performance Routines for Recovering Data from Solid State Drive During a Forensic Acquisition

by

Bhargav Rajammagari

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 Information Assurance

April, 2019

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

#### Abstract

The increased adoption rates of Solid-State Drives as the primary storage devices in digital computing is causing traditional computer forensic examination to face enormous challenges. Digital forensics has typical routines and guidelines which are followed to extract critical data in the form of evidence from storage drives of digital devices like computers and laptops. These conventional mechanisms apply to the traditional spinning media disk-based hard drives as these devices leave artifacts through which the forensic expert can extract and recover the deleted files. However, the Solid-State Drives make use of NAND based flash memory implementation which makes it impossible to recover the deleted data from these devices. Solid State Drives are unique in nature and architecture which is steered by a controller chip inside the device. The controller and algorithms are kept as a secret by the vendors of these devices which makes it impossible to retrieve data from these devices. It is necessary to examine the challenges that these devices pose in data recovery and to examine the possible methods for data recovery from these devices.

## **Table of Contents**

	Page
List o	f Tables5
List o	f Figures6
Chap	ter
I.	Introduction11
	Introduction11
	Problem Statement
	Nature and Significance of the Problem13
	Objective of the Project
	Project Questions
	Limitations of the Project14
	Definition of Terms14
	Summary15
II.	Background and Literature Review16
	Introduction16
	Background Related to Problem16
	Literature Related to Problem
	Literature Review Related to the Methodology
	Summary
III.	Methodology
	Introduction

pter Pa	age
Design of Study	.31
Data Collection	.31
Hardware and Software Requirements	.32
Timeline	.33
Data Presentation and Analysis	.34
Introduction	.34
Data Presentation	.34
Data Analysis	.55
Summary	.75
Results, Conclusion, and Recommendations	.76
Introduction	.76
Results	.76
Conclusion	.79
Future Work	.79
erences	.80

## List of Tables

Table	Page
1.	Project Timeline
2.	Comparison of Hits in HDD and SSD
3.	Comparison of File Hits in Various Images of Solid-State Drives77

## List of Figures

Figure	P	age
1.	The Usage of Solid-State Drives	12
2.	Hard Drive	18
3.	Solid-State Drive	21
4.	SSD NAND Flash Architecture	22
5.	Code Snippet for TRIM Functionality	26
6.	Wear Leveling	27
7.	Contents of Animal Folder	34
8.	Contents of Plant Folder	34
9.	Contents of Sunshine Folder	35
10.	Contents of Travel Folder	35
11.	Evidence and Junk Folders	35
12.	SSD and HDD Connected to a Computer	36
13.	Copying Evidence Files to SSD and HDD	36
14.	Contents of HDD and SSD	37
15.	Contents of HDD	37
16.	Junk Folders in HDD and SSD	38
17.	Passing Junk Folders in HDD and SSD	38
18.	Webpage for Downloading FTK Imager	39
19.	Registration Form for Downloading FTK Imager	39
20.	Email for Downloading FTK Imager	40

Figure	2	Page
21.	License Agreement for FTK Imager Download	40
22.	FTK Imager Installation Completed	41
23.	FTK Imager Welcome Page	41
24.	Selecting Source for FTK Imager	42
25.	Selecting Drive for FTK Imager	42
26.	Selecting Image Source	43
27.	Selecting Image Type	43
28.	Evidence Information Form	44
29.	Selecting Image Destination Location	44
30.	Creating Image	45
31.	Image Created	45
32.	Summary of Image Created	46
33.	SSD Images in Folder	46
34.	Selecting Source Type	47
35.	Selecting the Source Drive Selection	47
36.	Evidence Item Information	48
37.	Creating SSD Image 1	48
38.	License Agreement for Access Data FTK Suite	49
39.	FTK Suite Welcome Page	49
40.	Creating a New Case	50
41.	Forensic Examiner Information	51

Figure		Page
42.	Case Log Options	51
43.	Processes to Perform	
44.	Default Case Setting	
45.	Default Index Setting	53
46.	Adding Evidence	53
47.	Type of Evidence to Add	54
48.	Selecting Acquired Image	54
49.	Evidence Information	55
50.	Leaving Time Zone when Processing an Image 1	55
51.	First Image Results	56
52.	Sample Hits for Animals, Travel, and Plant for SSD Image 1	56
53.	Sample Hits for Sunshine, Travel, and Plant for SSD Image 1	57
54.	Sample Hits for .Doc and .Xlxs for SSD Image 1	57
55.	Sample Hits for .Doc, .Pdf, and .X1xs for SSD Image 1	58
56.	Creating a New Case for SSD Image 2	58
57.	Overview of SSD Second Image	59
58.	Hex Code of SSD Second Image	
59.	Sample Hits for Animals, Travel, and Plant for SSD Image 2	60
60.	Sample Hits for Sunshine, Travel, and Plant for SSD Image 2	60
61.	Sample Hits for .Doc and .Xlxs for SSD Image 2	61
62.	Sample Hits for .Doc, .Pdf, and .Xlxs for SSD Image 2	61

Figure		Page
63.	Creating a New Case for SSD Image 3	62
64.	Evidence Information for SSD Third Image	62
65.	Leaving Time Zone when Processing an Image 2	63
66.	Hex Code for SSD Third Image	63
67.	Sample Hits for Animals, Travel, and Plant for SSD Image 3	64
68.	Sample hits for sunshine, travel, and plant for SSD Image 3	64
69.	Sample Hits for .Doc and .Xlxs for SSD Image 3	64
70.	Sample Hits for .Doc, .Pdf, and .Xlxs for SSD Image 3	65
71.	Creating a New Case for SSD Image 4	65
72.	Evidence Information for SSD Image 4	66
73.	Leaving Time Zone when Processing an Image 4	66
74.	Hex Code for SSD Fourth Image	67
75.	Sample Hits for Animals, Travel, and Plant for SSD Image 4	68
76.	Sample Hits for Sunshine, Travel, and Plant for SSD Image 4	68
77.	Sample Hits for .Doc, .Pdf, and .Xlxs for SSD Image 4	69
78.	Sample Hits for Animals, Travel, and Plant for SSD Image 4	69
79.	Sample Hits for Animals, Travel, and Plant for HDD Image	70
80.	Sample Hits for Sunshine, Travel, and Plant for HDD Image	70
81.	Sample Hits for .Doc, .Pdf, and .Xlxs for HDD Image	71
82.	Total Number of Files Generated for HDD Image	71
83.	Image Preview for HDD Image	72

Figure		Page
84.	Image Preview 2 for HDD Image	72
85.	Image Preview 3 for HDD Image	73
86.	Excel Preview for HDD Image	73
87.	Document Preview for HDD Image	74
88.	Folders Hex Code for HDD Image	74
89.	Comparison of All Images vs. Recovered Data	78

#### **Chapter I: Introduction**

#### Introduction

Digital Forensic is the art of retrieving data from digital devices like computer, laptops, mobile phones, for evidence as a part of criminal investigation. Digital forensic helps in solving criminal cases by extracting data from various digital devices and using the data as evidence in solving a crime investigation. Due to its validity in the investigation, many commercial organizations have used the support of digital forensic for their benefits in various types of cases such as bankruptcy, espionage, fraud investigations, and intellectual property theft. Research has shown that nearly 95% of the criminal cases leave evidence which can be captured and analyzed through the computer and digital devices (Bell, 2010).

However, with the advancement in computer technology, new forms of storage devices have emerged. So far, most computing devices use the spinning media-based storage devices where data retrieval was done using a forensic kit; even if the data got permanently deleted. With the advancement in technology, Solid State devices have come into use as the primary storage for most of the digital computing devices. Solid State Devices do not leave behind any artifacts inside them and pose a massive challenge for the forensic data team to recover the data from these devices. Over the years, the adaptation rates of Solid-State Devices have been increasing due to the extended data security that it provides, and this has been posing severe challenges for the forensic science department. This work examines the technology available for data recovery of these devices and makes recommendations about future technologies (Chen, 2011). However, its usage has increased the complexity of forensic investigators. The TRIM, garbage collection and wear leveling creates sanitized disks which makes the data inaccessible for data recovery (Bednar & Katos, 2011).

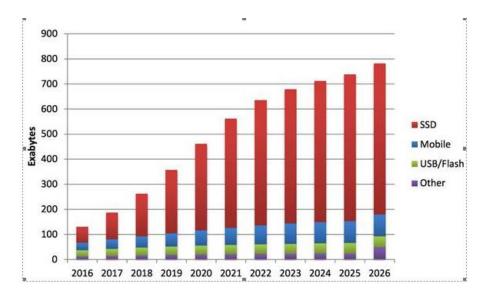


Figure 1. The Usage of Solid-State Drives (Geier, 2015)

Moreover, with each SSD, the garbage collection algorithm can vary in aggressiveness and can pose a severe complexity to the process of data recovery. It calls for an exploration of using various methods of data recovery that can be used by forensic experts on the solid-state drives. Based on these explorations, this work will examine the current state of the art of technology available for data recovery for these devices and will make a recommendation of future technologies (Bednar & Katos, 2011).

#### **Problem Statement**

Though SSDs are significantly fast in terms of speed compared to HDDs, Storage drives have brought revolution in terms of storage, which resulted in increased usage of this SSD. Storage drives raise a few challenges to digital forensic investigators, some of which are:

- 1. How can forensic analysis be done on SSD?
- 2. What routines are to be followed during a forensic analysis?
- 3. Which tools are used to perform the forensic analysis?
- 4. What type of data should we consider for this analysis?
- 5. How to compare the results between SSD and HDD?
- 6. How effective will the approaches be?

#### Nature and Significance of the Problem

The practices followed by digital forensic investigators to solve HDD data retrieval cases will be a lot easier and less challenging when compared SSD data retrieval because some SSDs are made using NAND flash memory.

As per the statistics shown in Figure1, we see a significant rise in the usage of SSD. So, the comparison of forensic analysis of HDD vs. SSD helps the researchers and investigators take better steps while doing a forensic analysis of SSD.

#### **Objective of the Project**

The research examines the complexity involved in SSD data recovery and the current state of the art of technology by analyzing the performance routines available in data recovery from these devices. The challenges forensic investigators face in extracting evidence during data recovery from the solid-state devices get easier when compared with hard disk drives.

#### **Project Questions**

The project questions are as follows:

1. What are the challenges faced by forensic investigators while using tools to retrieve information?

- 2. What type of files would be recoverable after deletion?
- 3. Would the deleted files be recoverable by other methods?
- 4. Can the results be the same with different approaches?

#### **Limitations of the Project**

The motive of this study is to examine challenges solid-state devices pose to the routines and mechanisms of forensic investigations. This study does not make any attempt to change any of the existing methods of extracting evidence or to the data recovery but suggests how these methods are adequate or not, for retrieving the data from these devices. The results obtained from this research might be valid only to this data.

#### **Definition of Terms**

*Digital forensics:* It is a process of interpreting and under covering electronic data. The primary goal of the digital forensics is performing a structured investigation by collecting, identifying and validating the digital information, so those past events are reconstructed while preserving any evidence in its most original form. Digital forensics can be very efficiently used in a court of law (Technopedia, n.d.).

*HDD:* A computer hard disk drive (HDD) is one of the mechanisms that steer the positioning, writing and reading of the disk. It is a non-volatile computer storage device which has magnetic disks or platters which are rotating at high speed. It acts as a secondary storage device. All the data stored non-volatilely are retained when the computer is turned off. Hard disk drives are also known as hard drives (Technopedia, n.d.).

*SSD*: Solid state drive (SSD) is an electronic storage drive built on solid-state architecture. SSD shares the same purpose as of Hard Disk Drive (HDD). NAND and NOR flash

memory are used to make SSDs and to store non-volatile data. SSD is also called as an electronic disk drive or Solid-State Drive (Technopedia, n.d.).

## Summary

In this chapter, we learned what HDD and SSD are and how they function, and how the market for SSDs is rapidly rising. We have also discussed the main problems faced by forensic experts for data retrieval in these devices. A brief description of the definition of terms also has been considered along with a short intro to study questions.

#### **Chapter II: Background and Literature Review**

#### Introduction

All the crimes related to computer technology and storage devices need digital forensic expertise to solve the crime investigation. A significant component of these storage devices is SSDs and HDDs. Retrieval of lost data from these storage devices is the primary job of a digital forensic investigator, especially when data retrieval from SSDs has become a difficult task. In this chapter, we will discuss why the data recovery process from SSD is different from that of HDD, and about the use of forensic tools with an in-depth functionality of HDD and SSD.

#### **Background Related to Problem**

Since SSDs have special features like TRIM function and wear leveling, and since they are made up of NAND flash memory, the techniques to study these behaviors and methods to extract data are very scarcely known. These features could be of significant advantage in fast in reading, write and store operations of SSDs, but possess a severe threat in the retrieval of deleted information.

#### **Literature Related to Problem**

**Forensics**. Digital forensics is a combination of elements in law with computer science and technology to analyze and collect data from computers, networks, wireless communications, and storage devices in such way that is acceptable as evidence in a court of law (Ries & Hill, 2017).

The field of digital forensics involves the exploration of digital data from digital devices as evidence for any case. The digital forensic thus collects and analyzes the data from computing devices like mobile, computer, laptops for obtaining evidence for a legal matter. For the past 30 years, this method has helped in solving various kinds of investigations for the public and the corporations as well. Digital forensics also includes the discovery of new information from digital computing devices which handle sensitive data. It also provides measures to ensure the data integrity, so that the confidential data cannot be corrupted by others and is intact for the evidence purpose (INFOSEC, n.d.).

It is through the digital forensics that many cases of fraud, theft, software privacy, software hacking, cybercrime, blackmailing, terrorism, prostitution, child pornography, domestic violence, trade secrets have investigated worldwide. Through digital forensics, cases of network intrusion, hacking, password hacking, cyber warfare, online trading frauds can also be examined from the computation device history and memory devices and can be used to recommend creating preventive applications to act as a safeguard against such crimes (INFOSEC, n.d.).

A few of the tools used in a forensic investigation are: (a) SANS SIFT, (b) Pro discover Forensic, (c), FTK, and (d) Autopsy (INFOSEC, n.d.).

**Spinning media drives and file storage (HDD).** Information in the computing devices is stored in the form of patterns of series of 1s and 0s. The 1s and 0s are used only for human interpretation but do not exist. The 1s and 0s signify the presence or the absence of electric charge or magnetism in the physical device. In today's computing devices, the main memory, which is often called as the Random-Access Memory stores the patterns of 1s and 0s by conducting charges in tiny battery like capacitors. To write the data into memory, some of these memory cells are identified and selected. These cells are filled with electric charge as per the data binary code. To read back the data from memory, the memory controller reads the electrical charge present in the cell, and the application program generates the binary value for the charge

stored in the memory cell. However, this storage of data in the form of charges poses a few issues. The primary problem being that the charge cannot be stored permanently, for an extended period. Hence it is necessary to read out the data and to recharge the memory cells to ensure that the data can be preserved in these drives. Such memory is called volatile memory. It makes use of a circuit to charge the memory cells and ensure that the data is stored in the device for an extended period. However, there are some non-volatile memories which can store the data for a permanent time without the need of the refreshing circuitry. These devices are called secondary storage devices, and the popular ones are the spinning media-based devices, i.e., the hard disk drive (Woodford, 2018).



*Figure 2*. Hard Drive (Phelps, 2012)

Previously commercial computers made use of spinning magnetic drum-based memories, which provide access to the data in the form of blocks of digital codes. These digital code blocks were written to and read from them randomly. It meant that the reading and writing from these devices in any order was helpful for the computer programs for smooth execution and eliminated the need for data to be read from any external storage devices from the beginning until the needed block found inside it. It also allowed changing the data on these storage devices through the process of re-writing the tracks of media. These Magnetic drums made use of the random organization of the data, and this helped in mapping the data to individual records of codes on the drum with clear information. Each of these tracks further divided into sectors (Woodford, 2018).

Slowly, this gave the concept of hard drives on the computer. Hard drives contain a shiny plate which is circular and has magnetic properties. This plate is known as the platter, and this is divided into small units of areas. These areas of platters can get magnetized independently and store the digital value equivalent to one or demagnetized values representing a value 0. It is through the concept of magnetization, the information is stored in these devices, even when there is no supply of power (Woodford, 2018).

These spinning platter-based storage devices replaced the traditional spinning drumbased storage drives. Slowly these evolved into spinning disks of magnetic media which are formatted with multiple tacks instead of the parallel magnetic drums. The track subdivision was known as sectors, and these sectors hold the data. For each of these drives, there was a moving read head or a write head that allows each platter to read/write data from or to any sector. While doing so some time was spent to reach to the correct track and correct sector. The time spent is called as seek time, and the delay for finding the first sector of the cluster by the read or write head is known as rotational latency of the drives (Woodford, 2018).

Over the years, the data to be stored on these drives started to increase, and this called for storage devices with increased size and increased capacity of the drives. It resulted in an organizational scheme of the file-based system where the approach was to store the data on these sectors in the form of files. This file-based system made use of a file allocation table, that gave the identification of the type of the file, its address, its permission, its ownership. The file allocation table also contained an index to the first cluster where the data of the file is present on the disk. In this scheme, a small amount of storage space was needed at the beginning of each sector to store index points which would link to the next sector to be used by that file (Woodford, 2018).

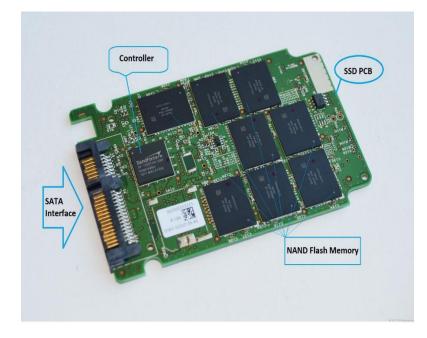
The hardware and software controllers worked in synchrony to access a file and lookup the desired data file from the file allocation table. It then followed a linked list of sector data to retrieve data from the file and use it for a program. When the file was not needed anymore on the disk, one of the approaches would be to overwrite the file by finding each sector allocated by that file through the file allocation table. However, this approach is not used by the hard disk. A faster method that reduces the wear and tears on the disk is used for altering the file allocation table, which is to show the entire files in the recovery area, so other programs use that. However, it is a standard practice to leave the deleted files intact, and this is used by the forensic experts and their tools to recover the data (Woodford, 2018).

**Mechanism of reading and writing in hard drives.** The process of storing data on hard drives is not much of a significant problem as compared to finding the data on these devices. The hard drives make use of a proper storage mechanism to store data in the tracks. For storing any information on the drives, the computer considers the file allocation table, which tells it about the independent sector information. After locating a free sector, the read-write head is moved to the sector area across the platters to store the data. For reading any data, the address for reading is obtained by the program. The address is located using the file allocation program and the read-

write head is moved to that address. The content from that sector is read, and the data is moved to data registers which were provided to the programs that need the data (Brendan, 2017).

**Solid state devices.** Solid State Devices are storage devices made up of NAND based flash memory chips where the data is read and written in the parallel form. The essential element in use in Solid State Devices is the NAND based flash memory which is semiconductor-based metal oxide memory. This memory is non-volatile and can provide enough density and speed for making this device to be a perfect device for the primary storage device (Bell, 2010).

SSDs makes use of a grid of cells which can send and receive any data. Pages separate the girds of the device, and it is in these pages where the data is stored. Pages are grouped to form blocks. In order to write data in SSDs, the page should be empty, and it avoids overwriting of the data (Wei, Grupp, Spada, & Swanson, 2011).



*Figure 3*. Solid-State Drive (C/net, n.d.)

The NAND flash chip components are stated in the figure. The flash page must be erased to make a write operation. However, the erasing mechanism takes a long time and can decrease the performance of the device (Wei et al., 2011).

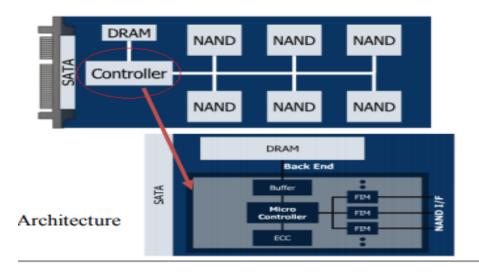


Figure 4. SSD NAND Flash Architecture (Thierolf & Uriarte, 2010)

The SSD central element the NAND flash poses several challenges to the SSD designers and manufacturers. Designers have increased the sensitivity of the read and write mechanism which gave rise to the Multi-Level Cell-based flash memory in SSD to increase the usage of solid state drives. Another issue was about to drive longevity due to the wear on the flash cells. This wear limited the erasing limits and the lifetime of the devices. It gave birth to the concept of wear leveling. It is through the wear leveling the block on the SSD is written once before any other writing to the block can be done again (Bux & Iliadis, 2010). Moreover, since the SSD makes use of the mechanism of reading data across all the chips at the same time, the need for a movable head has been eliminated. It results in no performance loss for the operation and wear leveling and has proven to be a valid concept for writing into the drives and increases its longevity (Chen, 2011). SSDs makes use of a feature known as Flash Translation layer which runs in SSD controller that can translate the block commands to execute on the flash. This feature blocks the software access to physical blocks on SSD (Bux & Iliadis, 2010). The translation acts as a mask to the flash hardware on the operating system. Through this translation, the operating system may be reporting that the blocks of the SSD may be unchanged, but the fact may be that the SSD might be reallocating the data on the drives (King & Vidas, 2011). In the mechanism of the garbage collection, the collector moves the active pages out of the block and performs the erase function on these blocks. As the writes are being carried out on new pages, the garbage collector and wear leveling has lead to the degradation of the performances as the garbage collector has to move between pages to keep the allocation pool filled. It gave birth to the TRIM function. TRIM changes disk garbage collection by allowing the operating system to mark blocks as deleted. TRIM changes disk garbage collection by allowing the operating system to mark blocks as deleted (King & Vidas, 2011).

**SSD operation**. The solid-state drives make use of flash memory like Random Access Memory (RAM), but the RAM is volatile and clears the data whenever the system power button is turned off. A solid-state drive, on the other hand, is non-volatile and retains the data even after the power loss (Chen, 2011). The solid-state drives make use of grid-based electrical cells for receiving data into the drives and sending data from the drives. Sections like pages separate these grids, and these pages hold the data of the drives. The pages are grouped to form blocks, and in solid-state drives, data is written into an empty page of the block. In Hard disk drives, the data can be written randomly to any location on the drive at any time signifying that data is overwritten, but in solid state drives data cannot be overwritten. For overwriting the data should be first written to some empty page and only then is that page used for writing the data. In solid state drives when there are enough unused pages, it will take the data of the block and commit that area of the memory to erase the whole block. Now the determined image will be printed on the block that has unused pages (Chen, 2011).

**Working of SSD.** The main two parts of the solid-state drives are its controller and the NAND flash memory. Along with other components, the whole circulatory for the solid-state drives is placed on a printed circuit board. The entire printed circuit board is placed in a casing and sold as solid-state drives (Chen, 2011).

The controller of the solid-state drives is a processor that is in the circuitry of the drives and act likes a bridge of the flash memory components and the host computer. The codes provided by the solid-state drive's firmware are executed by the controller which contains information to fulfill the requests of the hosts. It is the controller that shall decide how the solidstate drives should function and what features it should offer. The main functions which the controller controls and executes for the solid-state drives are read function, write function, error checking function, deletion function, garbage collection function, wear-leveling function, encryption function, overprovisioning function and the RAISE function (Chen, 2011).

The next important component of the solid-state drives is the NAND flash memory. The NAND flash memory is an integrated circuit which can store information. Single layer NAND flash memory is used in enterprise-based solid-state drives while the commercial solid-state drives make use of multilayer cell NAND flash memories. The single-layered solid-state drives are faster in nature, and the last longer which makes it expensive than the multilayer cell NAND flash memories. Writing operation in the solid-state drives takes place when the controller programs the cells of the memory for storing the data. The memory cell holds the voltage in the form of 1 or 0 and stores the data in the binary form (Chen, 2011).

Reading process in solid-state drives is pure as the controller does not much to do in reading, but the writing process in the solid-state drives is a very complicated process. The NAND flash memory cells are programmed for a time, and after that it becomes unreliable. This property of solid-state drives is known as write endurance or program-erase cycle. Wear leveling is used to reduce the impact of write endurance on the drive, which ensures the effective use of chips cells that can be used one by one.

The solid-state drives do not provide the easy overwriting of the old data as in hard disk drives, and this inefficiency makes the data management in solid-state drives trickier than the hard disk drivers. Data is written in the form of pages by pages and is erased through a block by block. When the data is deleted in solid-state drives like by empty recycle operation no erasing takes place. Windows operating system makes use of a TRIM command which marks the data for erasing as an invalid page. However, the actual erasing of the data takes place only when the user writes some new data into the drive. There shall be no writing in the solid-state drives without erasing the existing data first unless the solid-state drives are a fresh piece. For the old drive, the process of wear-leveling and garbage collection is executed to enable the drive to write the data into it (Chen, 2011). Due to garbage collection and wear-leveling data is re-written from one place to another and this process is known as the write amplification.

#### Literature Review Related to the Methodology

**TRIM.** This functionality is used to erase blocks that are marked to be deleted by the operating systems. It has negative impacts on data persistence and forensic analysis. After deletion, the data cannot be guaranteed as the memory controller of the SSD decides the when and the number of marked blocks to delete. It is an essential function of SSDs which is not available in HDDs. One of ATA Set management command attribute is TRIM. The operating system using TRIM will inform the block that is to be deleted on the SSD. TRIM gives the list of blocks which are safe for removal from the device. In Windows Server 2008 or Windows 7, the trim command is enabled by default. The user can manually disable the TRIM command (Geier, 2015).

Enable: fsutil behavior set disabledeletenotify 0 Disable: fsutil behavior set disabledeletenotify 1 Check the status of TRIM: fsutil behavior query disabledeletenotify Results explained below: DisableDeleteNotify = 1 (Windows TRIM commands are disabled) DisableDeleteNotify = 0 (Windows TRIM commands are enabled)

Figure 5. Code Snippet for TRIM Functionality (Geier, 2015)

**Garbage collection.** Garbage collection works closely with TRIM functionality. It keeps track of the cells that are to be deleted and combines extra data of empty ones which helps in removing other cells. Garbage Collection works in the background and will only work with TRIM command. If the file system instructs the memory to delete the address or if the LBA address maps to a new address, the page is removed immediately, but instead, it

is marked as deleted using TRIM command. The garbage collection keeps track of the files for removal. If all the files in the block are to be removed, the garbage collector erases the whole block. If most of the files in the block are to be removed, or if more empty blocks need to be created, the garbage collector moves the remaining items to different blocks and erases the complete block. This operation is performed in the background (Geier, 2015).

Wear leveling. Each NAND cell contains a limited lifespan and has a limited number of lifecycles and withstand more than 100000 cycles. Information is not always expected to get updated with the same frequency, some of which will take a longer time, and the other gets updated instantly. Maintaining the wearing out of cells is essential for the aging to be uniform and minimum. This process is called wear leveling. There are two approaches for wear leveling namely:

- Dynamic Leveling
- Static Leveling

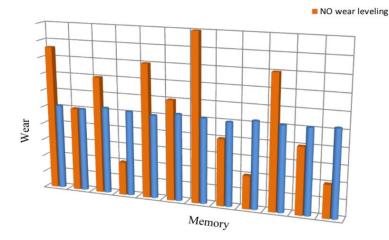


Figure 6. Wear Leveling (Geier, 2015)

Dynamic leveling is a technique of rampaging LBA address from one host system to the next available page. When the host updates the data, it either updates the page or writes into the drive. Data is always written into the next free cell with less aging level. Equal wearing is not guaranteed as unchanged cells will stay untouched (Geier, 2015).

Static leveling does the same functionality as dynamic leveling, but it also moves static pages to other pages periodically. Data in the oldest pages can be moved to an average aged page to make it usable for new data (Geier, 2015).

**Forensic investigation of spinning media drives.** Digital forensic experts rely on a few principles while examining the evidence from the spinning media devices. No harm should be done to the original media drive so that the integrity of the drive is preserved. To do so, the experts do not write anything on the drive but instead, make a backup copy of the drive and then perform the forensic analysis on the copy rather than on the original drive. Till date, a technique of dead box forensic was executed which considered the original drive as the Holy Grail and used other forensic tools to image the drive completely without altering its contents (Bednar & Katos, 2011).

**Forensic investigation of SSD devices.** The hardware of the solid-state devices, along with its firmware, exposes only those blocks of the device memory that are mapped to the sectors and attach it to the computer-based forensic applications. The forensic software examines the files which are allocated and are visible to the file system directory. Some of these files will be available in recycle bin. These are inactive files, and the fragments that are scheduled by the solid-state drive must be initialized to make them visible to the forensic analyzer software. It is found that the repeated usage of the forensic analysis software on the solid-state drives which is

recently formatted may show different results while being executed multiple times as these fragments reinitialize themselves. On the other hand, the repeated analysis by the forensic analyzer application on spinning media based hard disk drives generate same results, and the operation of this software on these hard disk drives is reliable and stable contrary to solid-state disk platforms (Zhao et al., 2013).

The solid-state drives create complexity in the data recovery due to two main processes. First through the implementation of the wear –leveling function, the data on the solid-state drives are not written in logical, sequential blocks but are scattered on the blocks of the device. In case any block fails then the file data is written to a different location which is unallocated in use. It makes the sequencing and addressing of these blocks a complex issue. These sequencing and addressing of the solid-state drive blocks are under the control of the manufacturer's algorithm and creates complexity for the forensic expert to get the file sequencing and to address. The other complication arises from the re-initialization of the deleted files quickly since the hardware blocks the initialization of the "blocks" before writing. Due to re-initialization, the contents of the erased data blocks remain in the solid-state drive for a brief period creating a challenge for the forensic experts to recover the data from the drive (Bell, 2010).

In an experiment, it was found that in 30 minutes, nearly 99% of the deleted files from the solid-state drives were wiped off and were not available for the forensic recovery. The deleted files in the solid-state drives are available only for a short period and these, when rewritten, make the deleted files to be unrecoverable for forensic experts. In research, it was found that the TRIM command enables commands to eliminate the deleted files from the drive and makes their recovery impossible but in the absence of the TRIM command, some portion of the data can be recovered (Bell, 2010).

Another challenge that the solid-state drives pose to the forensic experts is the encryption of the data at the device levels. Many third-party vendors and manufacturing companies provide a service of encryption of the disk data to preserve the integrity of the data on the drive. Due to encryption, the controller of the solid-state drives provide another level of abstraction for the original solid-state drives data and offers a cluster-based view of the data to the host computer. This abstraction creates complexity in forensic data recovery (Bell, 2010).

#### Summary

The study of this chapter shows the importance of SSDs and hard drives. It also shows the exact functioning of both. The advantages and disadvantages of SSDs and hard drives and the process of information storage in both also have been discussed in this chapter. The importance of SSD in the forensic examinations and the main components of the SSD such as NAND flash memory and controller are given in this chapter.

The main components of a hard drive also have been discussed. It can also present the need and importance of both the devices in today's world. The solid-state devices are unique and architecture. A controller chip inside the device controls them. It is this controller and the algorithms which are kept as a secret by the vendors of these devices. These controller and algorithms make it impossible to extract data from these devices. This study examines the main challenges the forensic investigators face in extracting evidence or data recovery from the solid-state devices and analyses the typical performance routines for recovering data from Solid State Drive during a forensic acquisition.

#### **Chapter III: Methodology**

#### Introduction

In this chapter, we discuss the methodology that we use to retrieve the deleted data using digital forensic techniques. The tools that we use for this process also will be addressed, and the comparison of results between SSD and HDD will be provided. We also discuss the hardware and software requirements on the machines or devices that have been used to perform the analysis.

#### **Design of the Study**

A laptop with Windows operating system is required. The primary motive of this experiment is to retrieve the deleted files in SSD and HDD using forensic tools. They are formatted before we use them. Load data into both the devices and remove them. We use FTK Imager to create images of the disks respectively. The images are taken at regular intervals of time and analyze those images with FTK tool kit. Check how many files have been recovered in SSD and HDD, compare the results.

#### **Data Collection**

Data collection process involves a laptop with an SSD and an HDD. Some specific set of files have been taken as evidence and passed on to the disks HDD and SSD respectively. Both these evidence files have been deleted. Now the garbage data to each of the disks has been passed again and has been removed.

Continued sending of garbage data to both the disks on specific timelines have been done and have been deleted. Now the disk images of HDD and SSD have been taken at regular intervals of time and analysis of these images and checks on the number of evidence files have

been retrieved in SSD and HDD is done, and the results are compared.

### Hardware and Software Requirements

Operating system Requirements: Windows & and above, i.e., 10 version

### Software Requirements:

- FTK Imager
- FTK tool kit
- HD Shredder
- Microsoft Office

## Hardware Requirements:

- Laptop Dell Inspiron 13 I7-7500U
- SSD 120 GB- Kingspec,
- HDD- 120 GB- Blueendless,

## Timeline

Table 1

## Project Timeline

Task	Duration
Selection of Topic by Reviewing Different Articles	Three weeks
Collecting Information Related to the Topic	Two weeks
Introduction and Literature Review	Three weeks
Review of the Document	One week
Project Proposal Documentation	One week
Collecting All the Resources for the Project	Three weeks
Creating Image Files and Analyzing the Image Files	Four weeks
Comparing and Analysis of Results	Three weeks
Documenting the Results	Two weeks
Project Defense Documentation and Presentation	Two weeks

#### **Chapter IV: Data Presentation and Analysis**

#### Introduction

Here we explain how the data has been collected by acquiring images of both external HDD and SSD. As a part of the next step, we will discuss on how we have extracted the data from the images acquired and how the comparison and analysis of the data have been performed along with the comparison of the results obtained from both the drives. The tools that have been used for this process are FTK imager and FTK.

#### **Data Presentation**

In this section, we would be discussing what type of files is present in the drives. There are different formats such as PDF, word documents, excel sheets. These have a high scope of evidence present in them as they might contain crucial information.

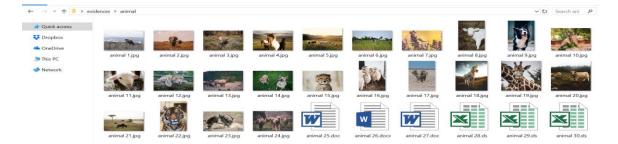


Figure 7. Contents of Animal Folder



Figure 8. Contents of Plant Folder

	evidences > sunshine									Search sun
Quick access							-			
Dropbox OneDrive		-			and the second second	- Autom		-	T. W	1 - marches
This PC	sunshine 1.jpg	sunshine 2.jpg	sunshine 3.jpg	sunshine 4.jpg	sunshine 5.jpg	sunshine 6.jpg	sunshine 7.jpg	sunshine 8.jpg	sunshine 9.jpg	sunshine 10.j
Network	-	-	-			L		Contraction of the second	-	
	and the second second		and the second second	and the second second	and the second		20.5	- Carlor		
	sunshine 11.jpg	sunshine 12.jpg	sunshine 13.jpg	sunshine 14.jpg	sunshine 15.jpg	sunshine 16.jpg	sunshine 17.jpg	sunshine 18.jpg	sunshine 19.jpg	sunshine 20,
			_							==1
	and the		and the state		W	W	TAT			
			Contraction of the second	and the second						
	sunshine 21.jpg	sunshine 22.jpg	sunshine 23.jpg	sunshine 24.jpg	sunshine 25.doc	sunshine 26.doc	sunshine 27.doc	sunshine 28.xls	sunshine 29.xls	sunshine 30

Figure 9. Contents of Sunshine Folder

Quick access Dropbox	<b>I</b> ST		and the	film.	24 A.L.	and the second	-		- Ale	
OneDrive				mal		CALL R	State State			
This PC	travel 1.jpg	travel 2.jpg	travel 3.jpg	travel 4.jpg	travel 5.jpg	travel 6.jpg	travel 7.jpg	travel 8.jpg	travel 9.jpg	travel 10.jp
Network		Series and a series of the ser	ACT-						and the	-
	travel 11.jpg	travel 12.jpg	travel 13.jpg	travel 14.jpg	travel 15.jpg	travel 16.jpg	travel 17.jpg	travel 18.jpg	travel 19.jpg	travel 20.jp
	C.A.	A.	Line.	W	W				W	
	travel 21.jpg	travel 22.jpg	travel 23.jpg	travel 25.doc	travel 26.doc	travel 27.xls	travel 28.xls	travel 29.xls	travel 30.doc	travel.jpg

Figure 10. Contents of Travel Folder

→ 👻 🕇 📕 > This PC > Bhargav (D	D:) ≯ junk	🗇 evidences, Pro	roperties ×
Quick access Dropbox OneDrive This PC Bhargav (D:) Network	junk 1	junk 3 General Customize Size All Location: All Size on disk: 11 Attributes:	

Figure 11. Evidence and Junk Folders

Evidence will be passed to HDD as well as SSD. The five Junk folders which have a wide variety of data like Excel sheets, PDF's, Images, MP3's with a size of 80GB will be copied to both.

First, we connect both SSD and HDD to the laptop, and we can see the preview as follows:

■   📝 📕 🖛   This PC File Computer \	View			
$\leftarrow \rightarrow \checkmark \uparrow > \uparrow$	•			
📌 Quick access	V Folders (7)			
🖿 Desktop 🛛 🖈		3D Objects	Desktop	Documents
👃 Downloads 🖈				
📔 Documents 🖈		Music	Pictures	Videos
🔚 Pictures 🛛 🖈				<b>Nideos</b>
Bhargav		121		
🧵 pdf	✓ Devices and drives (			
starred paper	-	OS (C:)	Bhargav ssd (D:)	Bhargav HDD (E:)
Study		777 GB free of 930 GB	119 GB free of 119 GB	111 GB free of 111 GB
ConeDrive				
🔄 This PC				

Figure 12. SSD and HDD Connected to a Computer

As a part of the next process, we copy all the evidence files and folders to both the HDD

and SSD, and we can see the action below:

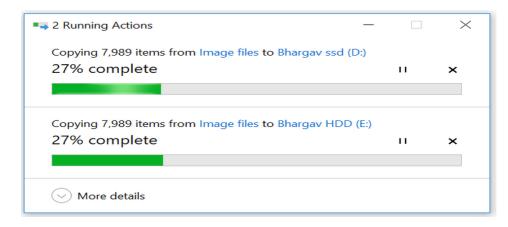
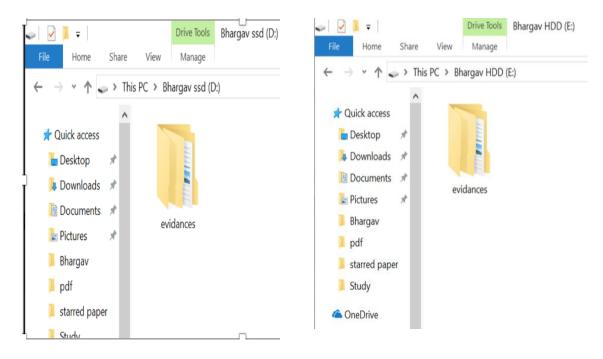


Figure 13. Copying Evidence Files to SSD and HDD

Evidence folder in SSD and HDD. We can see the evidence which is in the form of



files and folders in the SSD

Figure 14. Contents of HDD and SSD

As there are Five Junk Folders, they are passed into SSD and HDD with different

combinations as follows:

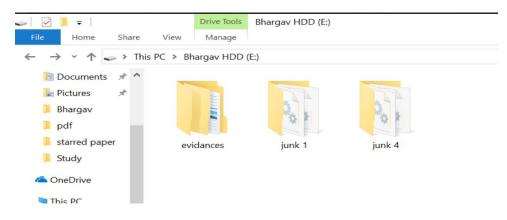
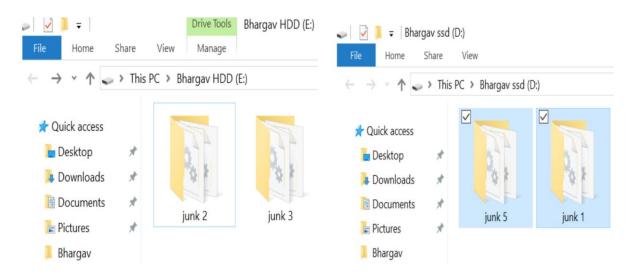


Figure 15. Contents of HDD



Delete the evidence and Junk folders and copying new Junk folders to HDD and SSD.

Figure 16. Junk Folders in HDD and SSD

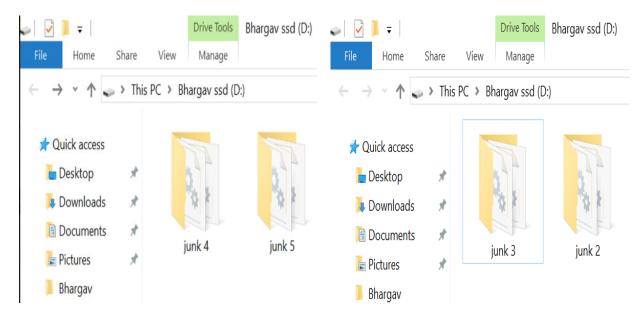


Figure 17. Passing Junk Folders in HDD and SSD

#### **Installation of FTK Imager.**

1. First, we go to https://accessdata.com/product-download/ftk-imager-version-4.2.0

and click on download now as follows:

	CARD OF T
HOME Product Downloads. FTK Imager	
» FTK Imager	
FTK IMAGER VERSION 4.2.0 Release Date: Dec 11, 2017	DOWNLOAD NOW

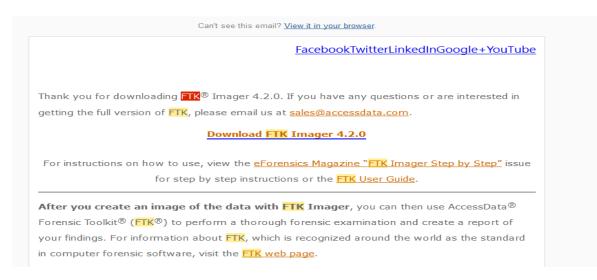
Figure 18. Webpage for Downloading FTK Imager

2. Then we need to fill in the form for getting the download link as follows:

To receive the download link, complete the information below
* First Name
Bhargav
* Last Name
Rajammagari
* Email
bhargavrajammagari@gmail.com
Phone
Country     United States
officed states
* State Minnesota
* Organization
St. Cloud State University
* Job Title
Student
* Organization Size
10,000+ ~
Organization Type
Student
AD Student Program
☑ Yes, I'd like to receive education updates from AccessData
via email
Graduation Year
Email Opt In
□ Yes*
Submit

Figure 19. Registration Form for Downloading FTK Imager

3. We can see the link which we received in the email as follows:



#### Figure 20. Email for Downloading FTK Imager

#### 4. Installation Steps after downloading the FTK.exe file:

RecessData FTK Imager - InstallShie	ld Wizard		×
License Agreement Please read the following license agree	ment carefully.		
END-USER LICENSE AG	REEMENT I FTWARE	FOR ACCESS	DATA
IMPORTANT-	READ CARE	FULLY	
This End-User License Agreemen between End User ("Licensee") (e juridical entity) and AccessData ( AccessData software that accomp associated media. AccessData Int	either an indivi Group, Inc. ("A panies this EUI	dual or a single AccessData'') fo LA, which inclu	e legal or for the edes
• I accept the terms in the license agreer			Print
○ I do not accept the terms in the license	agreement		
InstallShield			
	< Back	Next >	Cancel

Figure 21. License Agreement for FTK Imager Download

🕼 AccessData FTK Imager - In	stallShield Wizard $ imes$
	InstallShield Wizard Completed
	The InstallShield Wizard has successfully installed AccessData FTK Imager. Click Finish to exit the wizard.
	[✔] Launch AccessData FTK Imager
	< Back Finish Cancel

Figure 22. FTK Imager Installation Completed

Creating image of SSD. Now we open FTK imager and choose the source file for

selecting the SSD. We can see the preview as follows:

AccessData FTK Imager 4.2.0	0.13	_	٥	×
<u>File View M</u> ode <u>H</u> elp				
Evidence Tree	× File List			$\times$
	Name Size Type Date Mo			
Custom Content Sources Evidence:File System Path  Opt	Xons			^
Kew Edit Remove Remove A Properties Hex Value_Custom For User Guide, press F1				~

Figure 23. FTK Imager Welcome Page

Select the file and create a disk image option.

Please Select the Source Evidence Type
Physical Drive
O Logical Drive
O Image File
<ul> <li>Contents of a Folder (logical file-level analysis only; excludes deleted, unallocated, etc.)</li> </ul>
< Back Next > Cancel Help

Figure 24. Selecting Source for FTK Imager

Select Drive	$\times$
Source Drive Selection	
Please select from the following available drives:	
D:\ - Bhargav ssd [exFAT] ~	
Automate multiple removable media	
< Back Finish Cancel Help	<b>)</b>

Figure 25. Selecting Drive for FTK Imager

\\.\PHYSICALDRIVE1			
	Starting Evidence Number:	L	
Image Destination(s)			
Add	Edit	Remove	
Add	Edit Add Overflow Location	Remove	

## Figure 26. Selecting Image Source

Then we give in the evidence information for the image creation as follows:

Select Image Type		×
Please Select the Destination Image Type		
( Raw (dd)		
○ E01		
< Back Next >	Cancel I	Help

Figure 27. Selecting Image Type

Evidence Item Information	tion	$\times$
Case Number:	001	
Evidence Number:	001	
Unique Description:	Red color Z3 ssd	
Examiner:	Bhargav	
Notes:	SSD Image	
	< Back Next > Cancel Help	

Figure 28. Evidence Information Form

Image Source	
Select Image Destination	×
Image Destination Folder	_
C:\Images Browse	
Image Filename (Excluding Extension)	
001 - 2018	
Image Fragment Size (MB)       1500000         For Raw, E01, and AFF formats: 0 = do not fragment       0         Compression (0=None, 1=Fastest,, 9=Smallest)       0	
Use AD Encryption	

Figure 29. Selecting Image Destination Location

Then we can see the creation of an image as follows:

Creating Image.		_		$\times$	
Image Source:	\\.\PHYSICALDRIVE1				
Destination:	C:\SSD Images\001 - 2018				
Status:	Creating image				
Progress	Progress				
	osed time: 0:00:13 mated time left:				
	Cancel				

Figure 30. Creating Image

Then we can see that the image was created as follows:

Creating Image ×					
Image Source:	\\.\PHYSICALDRIVE1				
Destination:	C:\SSD Images\001 - 2018				
Status:	Image created successfully				
Progress	Progress				
	osed time: 0:31:43 mated time left:				
Image Summa	ry Close	]			

Figure 31. Image Created

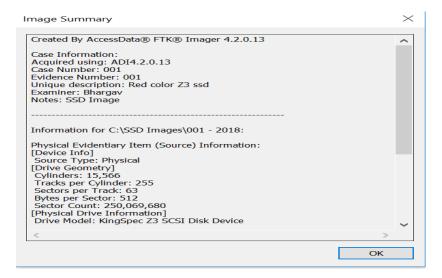


Figure 32. Summary of Image Created

SSD Image 2, Image 3, and Image 4 are constructed similarly.

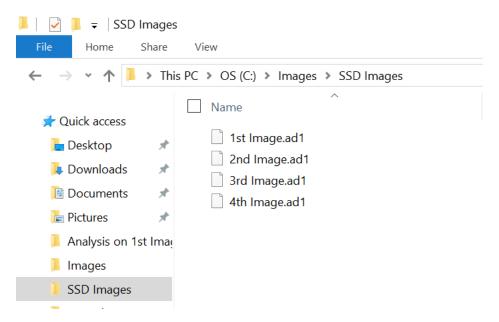


Figure 33. SSD Images in Folder

Creating image of HDD. As a part of the next process, we open the FTK Imager to

create the image of the HDD. We select the "Source evidence type" as Physical Drive.

Disease Calendation Calendary Trans
Please Select the Source Evidence Type
 Physical Drive
O Logical Drive
O Image File
<ul> <li>Contents of a Folder (logical file-level analysis only; excludes deleted, unallocated, etc.)</li> </ul>
< Back Next > Cancel Help

Figure 34. Selecting Source Type

Then in the next step, we choose the path for the available HDD, and we can see that in

the	image	below:
-----	-------	--------

Select Drive	$\times$
Source Drive Selection	
Please select from the following available drives:	
\\.\PHYSICALDRIVE1 - KESU USB 3.0 SCSI Disk Device [120GE	
< Back Finish Cancel	Help

*Figure 35*. Selecting the Source Drive Selection

After selecting the drive, we click on finish, and this proceeds to the creation of an image of the HDD. We see the information what we enter for the examination purpose as follows:

Evidence Item Information					
Case Number:	001				
Evidence Number:	001				
Unique Description:	hdd image1				
Examiner:	Bhargav				
Notes:	HDD image				
<	Back Next > Cancel Help				

Figure 36. Evidence Item Information

	Creating Image.			—	
	Image Source:		RIVE1		
1	Destination:	C:\Images\001	- 2018		
	Status:	Creating image.			
	Progress				
	Elapsed time: Estimated time left:		0:32:19		
			Cancel		

Figure 37. Creating SSD Image 1

As a part of the image creation, we can see the process as follows. Once it is done, we get an image of the HDD with all the contents of files and folders.

**Installation of access data FTK suite.** Access Data made forensic Tool Kit or FTK. It will scan a hard drive looking for different information. For example, to recover deleted emails, images. It also used to scan for text strings for using them as a password dictionary to crack the encryption.

cense Agreement			
ease read the following license agreement carefully,			
END-USER LICENSE AGREEMENT FO	OR ACCESSDATA S	SOFTWARE	^
IMPORTANT—READ	CAREFULLY		
his End-User License Agreement ("EULA") is a legal a tither an individual or a single legal or juridical entity) i te AccessData software that accompanies this EULA. w ternet based services ("Software"), and, any training nu company the Software. An annedment or addendum to ICENSEE AGREES TO BE BOUND BY THE TERM 'OPYING, OR USING THE SOFTWARE. IF LICENS' NSTALL, COPY, OR USE THE SOFTWARE, LICENS LACE OF PURCHASE FOR A FULL REPUND, IF AR	and AccessData Group which includes associa aterials and programs this EULA may acco s OF THIS EULA BY EE DOES NOT AGR SEE MAY RETURN I	p, Inc. ("Access ted media, Acco ("Program") that mpany the Soft INSTALLING EE, DOES NO	sData") for essData at ware. T
HIS SOFTWARE LICENSE ("EULA") ALLOWS THE dEDIA ("MEDIA") AND ACCOMPANYING USER D ONTAINED IN THIS PACKAGE. THIS EULA BET NCLUDING ITS SUCCESSORS OR ASSIGNS (REFEL UCENSOR") SUPERSEDES ANY PRIOP PROPOSA	OCUMENTATION ( WEEN LICENSEE AN RRED TO COLLECT	"DOCUMENT. ND ACCESSD. IVELY AS	ATION")
) I accept the terms in the license agreement			Print
) I do not accept the terms in the license agreement			
	< Back	Next >	Cancel

Figure 38. License Agreement for Access Data FTK Suite

After the installation:

File Items         B           tal File Rems:         0         B           hecked Rems:         0         E           agged Thumbnails:         0         D           ther Thumbnails:         0         F           Rered In:         0         C           Hered Out:         0         0	File Status FFAlert Files: 0 ookmarked items: 0 ad Extension: 0 ncrypted Files: 0 rom E-mail: 0 eleted Files: 0 rom Recycle Bir AccessDu uplicate items: AccessDu	Spreadsheets:     0       Databases:     0       Graphics:     0       Multimedia:     0	2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2	8 D 8		
File Items         B           tal File Rems:         0         B           hecked Rems:         0         E           agged Thumbnails:         0         D           ther Thumbnails:         0         F           Rered In:         0         C           Hered Out:         0         0	ookmarked Rems: 0 ad Extension: 0 ncrypted Files: 0 rom E-mail: 0 eleted Files: 0 rom Recycle Bir AccessD	Spreadsheets:     0       Databases:     0       Graphics:     0       Mutimedia:     0       E-mail Messages:     0				
tal Fieltems: 0 B necked items: 0 E tchecked items: 0 F agged Thumbnails: 0 D ther Thumbnails: 0 D ther double 0 D tered No. 0 D	ad Extension: 0 ncrypted Files: 0 rom E-mail: 0 eleted Files: 0 rom Recycle Bit AccessDi	Databases: 0 Graphics: 0 Multimedia: 0 E-mail Messages: 0	0 0 0			
ecked items:         0         E           checked items:         0         F           gged Thumbnails:         0         D           her Thumbnails:         0         F           ered In:         0         D           ered Out:         0         O	rom E-mail: 0 rom E-mail: 0 rom Recycle Bit AccessDi	Graphics: 0 Multimedia: 0 E-mail Messages: 0	D			
checked items:         0         Fr           agged Thumbnails:         0         D           her Thumbnails:         0         Fr           ered In:         0         D           ered Out:         0         O	rom E-mail: 0 eleted Files: 0 rom Recycle Bir AccessDa	Multimedia: 0 E-mail Messages: 0	D			
egged Thumbnails: 0 D her Thumbnails: 0 Friered In: 0 D ered Out: 0 D	eleted Files: 0 rom Recycle Bir AccessDa	E-mail Messages: 0				
her Thumbnails:         0         F           ered In:         0         D           ered Out:         0         O	rom Recycle Bir AccessDa		D			
ered In: 0 D ered Out: 0 O		ta FTK Startun				
ered Out: 0 O	uplicate items:			×		
	ce odolema.	& Analyse Computer Existence	Start a new case	ОК		
	lagged Ignore:		O Open an existing case	U.N.		
	FF Ignorable:			Cancel		
D	ata Carved File		O Preview evidence			3
8 88 48 🌨 🖻 🗅	) 😺 orr 🖬 두 🗗	rensic	O Go directly to working in program	m		
		Toolkit	O do uncerty to working in program			Children
Evidence File Name	Evidence Path				Added	Children
			Do not show this dialog on start			
			Do not show this dialog on start	up		

Figure 39. FTK Suite Welcome Page

To open and analyze a created image we need some software like FTK, Autopsy. In the below, I have a Forensic tool kit, and the First step is to select Start a New case and click OK. In the next level, we need to give the Investigator name. In this case, the investigator name is Bhargav. Case number refers to a unique number through which a case or investigation is assigned. The case name is the name of the case which we are about to investigate. Case path is giving the destination path, and case folder is the folder name to which the data must be stored.

Forensic		AccessData's Forensic Toolkit®-FTK® The Complete Analysis Tool	)
And Comparison Fundaments Toolkit		Wizard for Creating a New Cas	se
nvestigator Name: B	hargav	~	
Case Information	Case Number:	001 SSD	
	Case Name:	Analysis on 1st Image acquired from SSD	
	Case Path:	C:\Users\bharg\Desktop\starred paper\	Browse
Case Description:	Case Folder:	C:\Users\bharg\Desktop\starred paper\Analysis on 1st	Image acquire
I			~
			$\sim$

Figure 40. Creating a New Case

	FTK Report Wizard - Ca	se Information	$\times$	
le F ke		aminer Information n will appear on the Case Information page of the report:		_
ke n: ili ili ra v€	Agency/Company:	St Cloud State University		
il	Examiner's Name	Bhargav ~		
e) T	Address:			
ite				
gi ra	Phone:	Fax:		
	E-Mail:			_
¢	Comments:			
c				A
		< <u>B</u> ack <u>N</u> ext > Cance	I	

#### Figure 41. Forensic Examiner Information

To solve a case for a company or a university project, we need to mention that name. We

must fill up the personal details like email or phone number address.

Case Log Options	×
	Case Log Options
	ne case folder. It gets created automatically by FTK and contains a record of ise. You can choose which type of events you would like to be logged.
	log file at any time by selecting "Add Case Log Entry" under the "Tools" electing "View Case Log" under the "Tools" menu item.
Events to go in the Case Log	
Case and evidence events	Events related to the addition and processing of file items when evidence is added or when using Analysis Tools later in the case.
Error messages	Events related to any error conditions encountered during the case.
Bookmarking events	Events related to the addition and modification of bookmarks.
Searching events	Events related to searching. All search queries and resulting hit counts will be recorded.
Data carving / Internet searches	Events related to special data carving or internet keyword searches that are performed during the case.
Other events	Other events not related to the above, such as copying, viewing, and ignoring files.
	< <u>B</u> ack <u>N</u> ext > Cancel

Figure 42. Case Log Options

These are the options that we must consider while performing a forensic investigation. By

checking up the below fields, we can get the information about the errors and case events.

	Processes to Perform
	case in several steps. Some of the processes are always performed, while others are optional, ds and time/resource constraints.
MD5 Hash	An MD5 hash is a 16 byte value generated based upon a file's content. It is used to uniquely identify files. Hashes can be used to verify a file's integrity, or to identify duplicate files. MD5 hashes are used by the KFF to identify known files.
SHA1 Hash	A SHA1 hash is a 20 byte value. The SHA1 hashing algorithm is newer than MD5, but is not vet as widely used.
KFF Lookup	KFF (Known File Filter) is a utility that compares MD5 file hashes against a database of MD5 hashes from known files. The purpose of KFF is to eliminate files known to be unimportant, or to alert the investigator to known lifts or dangerous files.
Entropy Test	For unknown file types, an entropy test is used to determine whether the file's data is compressed or encrypted. Such files contain no plain text and will not be indexed. Unnecessary indexing of such files can wate large amounts of time and resources.
Full Text Index	The Forensic Toolkit includes a very powerful search engine, dtSearch, which enables the investigator to do instantaneous searching of textual data. In order to take advantage of this search feature the data must first be indexed.
Store Thumbnails	Create and store thumbnails for all graphics in the case. This option speeds up browsing through the Graphics view at the expense of consuming more space in the case folder.
Decrypt EFS Files	Automatically locate and attempt to decrypt EFS encrypted files found on NTFS partitions within the case. (Requires AccessData Password Recovery Toolkit 5.20 or newer)
File Listing Database	Create a Microsoft Access (Jet) database containing a list of all files in the case. The attribute included are based on the Preprocessing File Listing Database Column Setting. This databas can be recreated with custom column settings in Copy Special.
HTML File Listing	Create an HTML version of the File Listing.
Data Carve	Automatically find specific file types embedded in other files and from free space. Retrieve results using Data Carving Option on Tools Menu.
Registry Reports	Generate common registry reports during preprocessing.

Figure 43. Processes to Perform

It helps in including the filters and what perspective are we supposed to get the results.

m the case. Here, y ded to the case. To	ou can choose defau	It inclusion/exclusion se any changes to the sett	ttings that will apply to each	clude certain kinds of data ch evidence item that gets is that get excluded will not
Include All Items	Optimal Setting	s Email Empha	sis Text Emphasi	s Graphics Emphasis
Free Space (area KFF Ignorable Fil Extract files from Conditionally Add	as in the file system n es (files found by KFf KFF ignorable contai	ot currently allocated to to be forensically unimp ners		
Add other items to t		atisfy BOTH the file sta	tus and the file type ∨ File Type Criteria	criteria
Deletion Status: Deleted Not deleted Ether	Encryption Status: C Encrypted Not encrypted Ether	Email Status: O From email O Not from email Ether	Documents Spreadsheets Databases Graphics	Executables  Archives  Folders  Other Known
Include Du	plicate Files	OLE Streams	Multimedia	Unknown

Figure 44. Default Case Setting

We need to check either we need deletion status or encryption status and email status.

✓ Free Space (area	beyond the end of the as in the file system no les (files found by KFF	ot currently allocated to to be forensically unimp	· · ·	
Index other items in File Status Oriteria Deletion Status: O Not deleted Ether Include Du	Encryption Status: Encrypted Not encrypted Either	satisfy BOTH the file s Email Status: From email Not from email Ether OLE Streams	tatus and the file type          File Type Criteria          Ø Documents          Ø Spreadsheets          Ø Tatabases          Ø Graphics          Ø Hultimedia          Ø Email msgs	criteria Executables Archives Folders Other Known Unknown

Figure 45. Default Index Setting

Checking the boxes like file slack helps in viewing the data inside the file slack as well as

free spaces in the file system

dd Evidence to Case Any number of evidence items can be added to the case. There are several types of evidence items: Acquired image of drive: Several formats supported: can be an image of a logical or physical drive Local drive: Can be a logical or physical drive Merrice Can be a logical or physical drive Merrice Can be a logical or physical drive Merrice Can ddds al ifeige in the specified folder. including contents of subfolders Individual File: Adds a single file. NOTE: Disk image files should be added as acquired images. The default refinement options, set previously, can be overnidden independently for each evidence item, and additional types of orfinements can also be made. These refinements can include the exclusion of date/size ranges, as well as speci- folders. To make these further refinements, highlight an evidence item in the list and press Refine Evidence - Advanced Add Evidence	dd Evidence to Case							
Any number of evidence items can be added to the case. There are several types of evidence items:       Acquired image of drive: Several formats supported: can be an image of a logical or physical drive         Local drive:       Can be a logical or physical drive         Folder:       Adds all files in the specified folder, including contents of subfolders         Individual File:       Adds all files in the specified folder, including contents of subfolders         Individual File:       Adds all files in the specified folder, including contents of subfolders         The default findement options, set previously, can be overidden independently for each evidence item, and additional         Types of refinements can also be made. These refinements can include the exclusion of date/size ranges, as well as specificaters. To make these further refinements, highlight an evidence item in the list and press Refine Evidence - Advanced         Add Evidence       Edit Evidence       Remove Evidence       Refine Evidence - Advanced         Display Name       Source       Name/Nu       Type       Refined       Time Zone       Comment								
Any number of evidence items can be added to the case. There are several types of evidence items:       Acquired image of drive: Several formats supported: can be an image of a logical or physical drive         Local drive:       Can be a logical or physical drive         Folder:       Adds all files in the specified folder, including contents of subfolders         Individual File:       Adds all files in the specified folder, including contents of subfolders         Individual File:       Adds all files in the specified folder, including contents of subfolders         The default findement options, set previously, can be overidden independently for each evidence item, and additional         Types of refinements can also be made. These refinements can include the exclusion of date/size ranges, as well as specificaters. To make these further refinements, highlight an evidence item in the list and press Refine Evidence - Advanced         Add Evidence       Edit Evidence       Remove Evidence       Refine Evidence - Advanced         Display Name       Source       Name/Nu       Type       Refined       Time Zone       Comment			۷dd	Evic	lanca			
Acquired image of drive:       Several formats supported; can be an image of a logical or physical drive         Local drive:       Can be a logical or physical drive         Folder:       Adds all files in the specified folder, including contents of subfolders         Individual File:       Adds al single file.         NDTE:       Disk image files should be added as acquired images.         The default finement options, set previously, can be overridden independently for each evidence item, and additional types of refinements can also be made.         These refinements, highlight an evidence item in the list and press Refine Evidence - Advanced         Add Evidence       Edit Evidence.         Add Evidence       Edit Evidence         Display Name       Source         Name/Nu       Type         Refined       Time Zone         Comment	Anna an						3	
Local drive:       Can be a logical or physical drive         Folder:       Adda all files in the specified folder, including contents of subfolders         Individual File:       Adds all single file. NOTE: Disk image files should be added as acquired images.         The default refinement contasts set previously, can be overnidden independently for each evidence item, and additional yopes of refinements can also be made. These refinements can include the exclusion of date/size ranges, as well as specifolders. To make these further refinements, highlight an evidence item in the list and press Refine Evidence - Advanced         Add Evidence       Edit Evidence       Remove Evidence       Refine Evidence - Advanced         Display Name       Source       Name/Nu       Type       Refined       Time Zone       Comment								
Rolder:       Adds a lifes in the specified folder, including contents of subfolders         Individual File:       Adds a single file. NOTE: Disk image files should be added as acquired images.         The default refinement options, set previously, can be overidden independently for each evidence item, and additional types of refinements can also be made. These refinements can include the exclusion of date/size ranges, as well as specified folders. To make these further refinements, highlight an evidence tem in the list and press Refine Evidence - Advanced         Add Evidence       Edt Evidence       Remove Evidence       Refine Evidence - Advanced         Display Name       Source       Name/Nu       Type       Refined       Time Zone       Comment						a logical o	r physical drive	
The default refinement options, set previously, can be ovenidden independently for each evidence item, and additional spes of refinements can also be made. These refinements can include the exclusion of date/size ranges, as well as specioders. To make these further refinements, highlight an evidence term in the list and press Refine Evidence - Advanced           Add Evidence         Edit Evidence         Remove Evidence         Refine Evidence - Advanced           Display Name         Source         Name/Nu         Type         Refined         Time Zone         Comment		Adds all files in	the spe	ecified fol	der, including co			
types of refinements can also be made. These refinements can include the exclusion of date/size ranges, as well as specifolders. To make these further refinements, highlight an evidence item in the list and press Refine Evidence - Advanced         Add Evidence       Edt Evidence       Remove Evidence       Refine Evidence - Advanced         Display Name       Source       Name/Nu       Type       Refined       Time Zone       Comment		-			-			-
Display Name Source Name/Nu Type Refined Time Zone Comment	types of refinements can al	lso be made. These ref	finemen	nts can in	clude the exclusion	sion of date	e/size ranges, a	as well as speci
	Add Evidence	Edit Evidence		Rem	ove Evidence	Ref	fine Evidence ·	Advanced
< Back Next > Cancel	Display Name	Source	Nam	e/Nu	Туре	Refined	Time Zone	Comment
< Back Next > Cancel								
< Back Next > Cancel								
< Back Next > Cancel								
< Back Next > Cancel								
< Back Next > Cancel								
< Back Next > Cancel								
< Back Next > Cancel								
< <u>Back</u> Next > Cancel								
< Back Next > Cancel								
< Back Next > Cancel								
< <u>Back</u> Next > Cancel								
< <u>B</u> ack <u>N</u> ext > Cancel								
< <u>Back</u> Next > Cancel								
< <u>B</u> ack <u>N</u> ext > Cancel								
< <u>B</u> ack <u>N</u> ext > Cancel								
< Back Next > Cancel								
< <u>B</u> ack <u>N</u> ext > Cancel								
< <u>B</u> ack <u>N</u> ext > Cancel								

Figure 46. Adding Evidence

We can add the Created image as an evidence

Add Evidence to Case			)	×
1	Add Evidence			
Any number of eviden	ce items can be added to the case. There are several types of evidence ite	ms:		
Acquired imag Local drive: Folder: Individual File	ye of drive: Several formats supported; can be an image of a logical or phys Can be a logical or physical drive Adds all files in the specified folder, including contents of subfolk Adds a single file. NOTE: Disk image files should be added as a added as a single file. Note: Disk image files should be added as a single file. Note:	ders	mages.	
	options, set previously, can be ovenidden independently for each evidence			
types of refinements c folders. To make these	Add Evidence to Case ×		s well as specif - Advanced	IC
Add Evidence	Type of Evidence to Add to Case	Jence -	Advanced	
Display Name	Acquired Image of Drive	Zone	Comment	
	○ Local Drive			
t	○ Contents of a Folder			
t	$\bigcirc$ Individual File			7
	Continue Cancel			
				_
				-
	< <u>B</u> ack <u>N</u> e	xt >	Cancel	

Figure 47. Type of Evidence to Add

Select the acquired image of the drive and select continue.

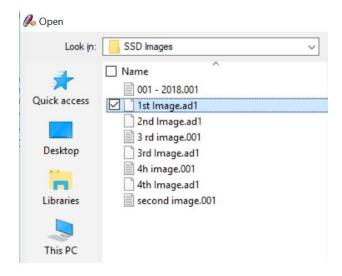


Figure 48. Selecting Acquired Image

# Data Analysis

Select Image 1 and open the image.

C:\Images\SSD	Images\1st Image	.ad1	
Evidence Displ	ay Name:		
1st Image			
Evidence Identi	fication Name/Nun	nber:	
1st image - SS	D		
Comment:			
Local Evidence	Time Zone:		

## Figure 49. Evidence Information

Leave comments and the time zone we are staying

lmages\SSD	lmages\1st lmage.ad1		
rrent File Iten	1:		
t Image\ (2)\N	IONAME-Unknown\DriveFreeSpace	0287	
urrent File Ite	m Status	Total Process Status	
Action:	Filtering Text	Elapsed Time:	0.00:02:19
File	Drive Free Space	Total Items Examined:	300
ltem	26,214,400 (287 of 4877)	Total Items Added:	300
Progress:	23,326,720	Total Items Indexed:	3

Figure 50. Leaving Time Zone when Processing an Image 1

Edit View	Tools H	Help																
Overview	Explo	ire (	Braphics	E-Mail	Search	h Bo	okmark											
Evidence It	ems	File S	tatus	File Categ	jory		~ A. 1	n 🐺 🖬 📾 🗿 🏹	<b>6</b>									
Evidence Items:	3	KFF Alert File	s: 0	Documents:	0			0 00 00 00-00 00 0	1.00	00.00								
File Item	15	Bookmarked	tems: 0	Spreadsheets:	0			0 00 00 00-00 00 0										
Total File tems:	4896	Bad Extensio	n: 0	Databases:	0			0 00 00 00-00 00 0										
Checked items:	0	Encrypted Fil	es; O	Graphics:	0	0000030 0	0 00 00 00 0	0 00 00 00-00 00 0	0 00 00 00	00 00 -								
Unchecked Items	4896	From E-mail:	0	Multimedia:	0	0000040 0	0 00 00 00 0	0 00 00-00 00 00 0	0 00 00 00	00 00 .								
Flagged Thumbru	ails: 0	Deleted Files:	0	E-mail Messages	к 0			0 00 00 00-00 00 0		00 00 -								
Other Thumboals	s: 0	From Recycle	Bin: 0	Executables:	0			0 00 00 00-00 00 0										
Filtered In:	4896	Duplicate iten		Archives:	0		0 00 00 00 00 0											
Filtered Out	0	OLE Subitem		Folders	1			0 00 00 00-00 00 0										
	Filtered	Flagged Ignor		Slack/Free Space	e: 4895			0 00 00 00-00 00 0										
	ctual Files	KFF Ignorable		Other Known Ty														
Allectrics	ciuairiica	Data Carved		Unknown Type:	0	Cursor pos	ition = 0: clu	ster = 204800; logic	al sector =	204800:	physical	sector	= 61644	18				
			Charles and the second		All Colu		V DIZ	I.Site	D.Site	Children	Dercen	For	Dal Re	0/2	Cer 1	de la	Sector	Clue
Ext File T	Туре	Category	Unfiltered Subject	Cr Date	Mod	umns iDate	Acc Date	L-Size	P-Size	Children	Descen	Enc	Del Re	cyc		dx	Sector	Clus
Ext File T Root	Type Folder		Charles and the second		11.0 [[]]			L-Size 612 612	P-Size 512 512	Children 12 0	Descen 12 0	Enc	Del Re	cyc	F	ldx Sull	Sector 6,374 250.069.6	Clus
Ext File T Root I File 1	Type Folder system	Category Folder	Charles and the second	Cr Date N/A	Mod N/A		Acc Date	512	512	12	12	Enc	Del Re	cyc	F	ull	6,374	Clus
Ext File 1 Root File s File s	Type Folder system	Category Folder Slock/Free S	Charles and the second	Cr Date N/A N/A	Mod N/A N/A		Acc Date N/A N/A	512 512	512 512	12 0	12 0	Enc	Del Re	cyc	F	ull ull	6,374 250,069,6	Clus
Ext File 1 Root 1 File 3 File 3 Drive	Type Folder system Free S	Category Folder Slack/Free S Slack/Free S	Charles and the second	Cr Date N/A N/A N/A	Mod N/A N/A		Acc Date N/A N/A N/A	512 512 10,384	512 512 16,384	12 0 0	12 0 0	Enc	Del Re	cyc	F	iuli iuli iuli	6,374 250,069,6	Clus
Ext File 1 Root 1 File 3 File 3 Drive Drive	Type Folder system Free S Free S	Category Folder Slack/Free S Slack/Free S Slack/Free S	Charles and the second	Cr Date NA NA NA NA	Mod N/A N/A N/A		Acc Date N/A N/A N/A N/A	512 512 10,384 26,214,400	512 512 10,384 127,824,5	12 0 0	12 0 0	Enc	Del Re	cyc	FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF	iuli iuli iuli	6,374 250,069,6	Clust
Ext File 1 Root I File s File s Drive Drive Drive Drive	Type Folder system free S Free S Free S Free S	Category Folder Slack/Free S Slack/Free S Slack/Free S Slack/Free S Slack/Free S	Charles and the second	Cr Date N/A N/A N/A N/A N/A N/A	Mod NA NA NA NA NA NA		Acc Date N/A N/A N/A N/A N/A N/A N/A	512 512 10.384 20.214.400 20.214.400 20.214.400 20.214.400	512 512 16,384 127,824,5 127,824,5 127,824,5 127,824,5	12 0 0 0 0 0 0	12 0 0 0 0 0 0	Enc	Del Re	cyc	F F F F F	Full Full Full Full Full Full	6,374 250,069,6	Clust
Ext File 1 Root 1 File 3 Prive Drive Drive Drive Drive	Type Folder system free S Free S Free S Free S Free S	Category Folder Slack/Free S. Slack/Free S. Slack/Free S. Slack/Free S. Slack/Free S. Slack/Free S.	Charles and the second	Cr Date NA NA NA NA NA NA NA NA	Mod N/A N/A N/A N/A N/A N/A		Acc Date N/A N/A N/A N/A N/A N/A N/A N/A	612 512 16,384 26,214,400 26,214,400 26,214,400 26,214,400 20,214,400	512 512 16,384 127,824,5 127,824,5 127,824,5 127,824,5 127,824,5	12 0 0 0 0 0 0 0	12 0 0 0 0 0 0 0	Enc	Del Re	cyc	F F F F F F	Full Full Full Full Full Full	6,374 250,069,6	Clust
Ext File 1 Root 1 File 3 File 3 Drive Drive Drive Drive Drive Drive Drive	Type Folder system Free S Free S Free S Free S Free S	Category Folder Slady Free S Slady Free S	Charles and the second	Cr Date NA NA NA NA NA NA NA NA	Mod N/A N/A N/A N/A N/A N/A		Acc Date N/A N/A N/A N/A N/A N/A N/A N/A	812 512 10.384 26.214.400 26.214.400 26.214.400 26.214.400 26.214.400 26.214.400	512 512 10,384 127,824,5 127,824,5 127,824,5 127,824,5 127,824,5 127,824,5	12 0 0 0 0 0 0 0 0 0 0	12 0 0 0 0 0 0 0 0 0 0 0 0	Enc	Del Re	cyc	F F F F F F	Full Full Full Full Full Full Full	6,374 250,069,6	Clust
Ext File 1 Root 1 File 3 File 3 Drive Drive Drive Drive Drive	Type Folder system Free S Free S Free S Free S Free S Free S	Category Folder Slack Free S. Slack Free S.	Charles and the second	Cr Date NA NA NA NA NA NA NA NA	Mod NA NA NA NA NA NA NA		Acc Date N/A N/A N/A N/A N/A N/A N/A N/A	512 512 512 512,26,214,400 26,214,400 26,214,400 26,214,400 26,214,400 26,214,400	512 512 16.384 127.824.5. 127.824.5. 127.824.5. 127.824.5. 127.824.5. 127.824.5.	12 0 0 0 0 0 0 0 0 0 0 0 0 0 0	12 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	Enc	Del Re	cyc	F F F F F F F F F F F F F F F F F F F	Full Full Full Full Full Full Full Full	6,374 250,069,6	Clust
Ext File 1 Root 1 File 3 File 3 Drive Drive Drive Drive Drive	Type Folder ystem Free S Free S Free S Free S Free S Free S Free S Free S	Category Folder Slack Free S. Slack Free S.	Charles and the second	Cr Date N/A N/A N/A N/A N/A N/A N/A N/A N/A	Mod N/A N/A N/A N/A N/A N/A N/A N/A		Acc Date N/A N/A N/A N/A N/A N/A N/A N/A	512 512 16,384 28,214,400 28,214,400 28,214,400 28,214,400 28,214,400 28,214,400 28,214,400 28,214,400	512 512 16.384 127.824,5. 127.824,5. 127.824,5. 127.824,5. 127.824,5. 127.824,5. 127.824,5.	12 0 0 0 0 0 0 0 0 0 0 0 0	12 0 0 0 0 0 0 0 0 0 0 0 0 0 0	Enc	Del Re	cyc	F F F F F F F F F F F F F F F F F F F	Full Full Full Full Full Full Full Full	6,374 250,069,6	Clus
Ext File 1 Root 1 File 3 File 3 Drive Drive Drive Drive Drive Drive Drive Drive	Type Folder ystem ystem Free S Free S Free S Free S Free S Free S Free S Free S	Category Folder Sladk Free S. Sladk Free S.	Carlos and a second	Cr Date N/A N/A N/A N/A N/A N/A N/A N/A N/A N/A	Mod N/A N/A N/A N/A N/A N/A N/A N/A		Acc Date N/A N/A N/A N/A N/A N/A N/A N/A N/A N/A	512 512 10.384 28,214,400 28,214,400 28,214,400 28,214,400 28,214,400 28,214,400 28,214,400 28,214,400 28,214,400	512 512 16.384 127.824.5. 127.824.5. 127.824.5. 127.824.5. 127.824.5. 127.824.5. 127.824.5. 127.824.5.	12 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	12 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	Enc	Del Re	cyc	F F F F F F F F F F F F F F F F F F F	Full Full Full Full Full Full Full Full	6,374 250,069,6	Clus
Ext File 1 Root 1 File 3 File 3 Drive Drive Drive Drive Drive Drive Drive Drive Drive	Type Folder ystem ystem Free S Free S Free S Free S Free S Free S Free S Free S	Category Folder Slack Free S. Slack Free S.	Carlos and a second	Cr Date N/A N/A N/A N/A N/A N/A N/A N/A N/A	Mod N/A N/A N/A N/A N/A N/A N/A N/A		Acc Date N/A N/A N/A N/A N/A N/A N/A N/A	512 512 10.384 20.214.400 20.214.400 20.214.400 20.214.400 20.214.400 20.214.400 20.214.400 20.214.400 20.214.400	512 512 10.384 127.824.5. 127.824.5. 127.824.5. 127.824.5. 127.824.5. 127.824.5. 127.824.5. 127.824.5. 127.824.5. 127.824.5.	12 0 0 0 0 0 0 0 0 0 0 0 0	12 0 0 0 0 0 0 0 0 0 0 0 0 0 0	Enc	Del Re	cyc	F F F F F F F F F F F F F F F F F F F	Full Full Full Full Full Full Full Full	6,374 250,069,6	Clus
Ext File I Root I File I File I Drive Drive Drive Drive Drive Drive Drive Drive Drive Drive	Type Folder ystem Free S Free S	Category Folder Slack/Free S. Slack/Free S.	Carlos and a second	Cr Date N/A N/A N/A N/A N/A N/A N/A N/A N/A N/A	Mod N/A N/A N/A N/A N/A N/A N/A N/A N/A		Acc Date NA NA NA NA NA NA NA NA NA NA NA NA NA	512 512 10.384 28,214,400 28,214,400 28,214,400 28,214,400 28,214,400 28,214,400 28,214,400 28,214,400 28,214,400	512 512 16.384 127.824.5. 127.824.5. 127.824.5. 127.824.5. 127.824.5. 127.824.5. 127.824.5. 127.824.5.	12 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	12 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	Enc	Del Re	cyc	F F F F F F F F F F F F F F F F F F F	Full Full Full Full Full Full Full Full	6,374 250,069,6	Clus
Ext File 1 File 1 File 3 Drive Drive Drive Drive Drive Drive Drive Drive Drive Drive Drive Drive	Type Folder ystem ystem Free S Free S	Category Folder Slack/Free S. Slack/Free S.	Carlos and a second	Cr Date N/A N/A N/A N/A N/A N/A N/A N/A N/A N/A	Mod NA NA NA NA NA NA NA NA NA NA NA		Acc Date NA NA NA NA NA NA NA NA NA NA NA NA NA	512 512 10.384 28.214.400 28.214.400 28.214.400 28.214.400 28.214.400 28.214.400 28.214.400 28.214.400 28.214.400	512 512 16.334 127.824,5. 127.824,5. 127.824,5. 127.824,5. 127.824,5. 127.824,5. 127.824,5. 127.824,5. 127.824,5. 127.824,5.	12 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	12 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	Enc	Del Re	cyc	F F F F F F F F F F F F F F F F F F F	Full Full Full Full Full Full Full Full	6,374 250,069,6	Clus

This process will take approximately five to six hours to analyze the image.

Figure 51. First Image Results

Results of the first image. Now in the Search Term box, we search for indexed Words.

From the below image we can see a sample number of hits for the search items animals, travel,

plant, and sunshine.

Overview	1	Explore	0	Graphics	E-Mail		565	arch	
Indexed Search	Live	Search							
Search Term:					Add	Impo	ort	Option	IS
Indexed Wo	rds (	Co	Search Ite	ems			Hits	Files	^
			animal				249	42	
			travel				763	95	Т
			plant				426	33	~
			<					>	
			Edit Item	Remove Ite	Remove Al	V	/iew Iter	n <mark>Resul</mark> t	s »
			Cumulative (	operator: AN	ID OR Vie	ew C	umulativ	e Result	ts »

AccessData FTK 1.81.0 DEMO VERSION -- C:\Users\bharg\Desktop\starred paper\Analysis or

Figure 52. Sample Hits for Animals, Travel, and Plant for SSD Image 1

Overview		Explore	Graphics	E-Mail		Sea	arch	
Indexed Searc	h Live	Search						
Search Term:				Add	Imp	ort	Option	IS
Indexed Wo	ords	Co	Search Items			Hits	Files	1
			travel			763	95	
			plant			426	33	I
			sunshine			37	14	•
			<				>	
			Edit Item Remove	e Item Remove	All \	/iew Iten	n Result	s
			Cumulative operator:	AND OR	View C		e Resul	to.

🔏 AccessData FTK 1.81.0 DEMO VERSION -- C:\Users\bharg\Desktop\starred paper\Analysis o

Figure 53. Sample Hits for Sunshine, Travel, and Plant for SSD Image 1

Now we search for .doc, .pdf, and .xlxs files, and we see the number of hits as follows.

Overview	Explo	re	Graphics	E-Mail	Sea	arch
Indexed Sear	ch Live Sear	ch				
Search Term				Add	Import	Options
Indexed W	ords Co	Sear	ch Items		Hits	Files
		.doc			584	1498
		.xlxs			399	366
		Cum	nulative Results (u	sing OR)	588	1744
		Edit	Item Remove Ite	Remove All	View Iter	n Results »
		Cumula	ative operator: AN	ID OR View	w Cumulativ	e Results »
ň	~ M_	<u> </u>	🛐 🔀 🔀	<u>F</u>		

🐊 AccessData FTK 1.81.0 DEMO VERSION -- C:\Users\bharg\Desktop\starred paper\Analysis on

Figure 54. Sample Hits for .Doc and .Xlxs for SSD Image 1

		View											
	Overvie	ew	ł	Explore		Gra	aphics		E-Mail		Se	arch	
In	dexed	Search	Live	Search	1								
S	Search	Term:						ł	Add	Imp	ort	Option	IS
	Index	ed Word	ds (	Co	Sea	arch Item	ns				Hits	Files	^
					.do	c					584	1498	
					.xlx	s					399	366	
					.pd	lf					161	1726	~
					<							>	
					Ed	lit Item	Remove	ltem	Remove	All	View Iter	m Result	s »
					Cumu	ulative op	erator: 🖌	AND	OR	View 0	Cumulativ	e Resul	ts »
ø	6			8 I	a 🖂	් සුම සු	à 🚗 🔽	n 🔊					
•	•		~	w   J	⊷ 🚔		È 🙆 🖸	2					

AccessData FTK 1.81.0 DEMO VERSION -- C:\Users\bharg\Desktop\starred paper\Analysis or

Figure 55. Sample Hits for .Doc, .Pdf, and .Xlxs for SSD Image 1

Analysis for second image of SSD. Now we fill in the case information such as Case

Number, Case Name, Case Path, and Case Folder and click on next.

Egrensic		AccessData's Forensic Toolkit®-FTK The Complete Analysis Too	-
The Company and Easty Toolkit		Wizard for Creating a New Ca	ase
nvestigator Name: 🔋	hargav	~	
Case Information			_
	Case Number:	002 SSD	
	Case Name:	Analysis on 2nd Image acquired from SSD	
	Case Path:	C:\Users\bharg\Desktop\starred paper\	Browse
Case Description:	Case Folder:	C:\Users\bharg\Desktop\starred paper\Analysis on 2	2nd Image acquir
			^

Figure 56. Creating a New Case for SSD Image 2

Edit View Tools Overview Expl				-								
are provided in the second sec			E-Mail	Sear	ch Bookn							
Evidence Items	File Status		File Categor		, m	~	🔊 ) 🖂 🙀	स्ति सिंहे 😣 🧯	2] 🥭			
vidence Items: 3		0	Documents:	0								-
File Items	Bookmarked Items:	0	Spreadsheets:	0								
otal File Items: 4896		0	Databases:	0								
hecked Items: 0		0	Graphics:	0								
nchecked Items: 4896	From E-mail:	0	Multimedia:	0								
lagged Thumbnails: 0		0	E-mail Messages:	0								
ther Thumbnails: 0		0	Executables:	0								
ittered In: 4896		4	Archives:	0								
ittered Out: 0		0	Folders:	1								
Unfiltered Filtered	Flagged Ignore:	0	Slack/Free Space:	4895								
All Items Actual Files		0	Other Known Type									
	Data Carved Files:	0	Unknown Type:	0	<							>
8 88 🛷 😫 🖪		-	~ []		olumns	~	DTZ					
File Name	a 🗋 🐳 off Unfilter Full Path	ed	ystem Partition (1)/EF		Recycle Bi		DTZ File Type Root Folder	Category Folder	Subject	Cr Date N/A	/lod Date /A	
E BB (& 😪 (1) File Name C File Root Folder]	a 🗋 🐳 off Unfilter Full Path	ed					File Type		Subject			
File Name	a 🗋 🐳 off Unfilter Full Path	ed					File Type		Subject			
File Name	a 🗋 🐳 off Unfilter Full Path	ed					File Type		Subject			
File Name	a 🗋 🐳 off Unfilter Full Path	ed					File Type		Subject			
File Name	a 🗋 🐳 off Unfilter Full Path	ed					File Type		Subject			
File Name	a 🗋 🐳 off Unfilter Full Path	ed					File Type		Subject			
File Name	a 🗋 🐳 off Unfilter Full Path	ed					File Type		Subject			
File Name	a 🗋 🐳 off Unfilter Full Path	ed					File Type		Subject			

Now when we click on the overview, we can see 4896 items.

Figure 57. Overview of SSD Second Image

We can see the Hex code format for one of the selected files as follows:

Overview Expl	Help Graphics	E-Mail	Sear	- 1	Bookmark							
LAPS.					BOOKMARK		1					
Evidence Items	File Status	File Cate		M		-	, po 📥 🕴	स्त्रे 🗃	O] 🐔			
Evidence Items: 3	KFF Alert Files: 0	Documents:	0	0000	000 c7 6c	7f 8	d 2e 57 6	e 7a-1c 7	7 fa f7 ab 6	9 ee 4c C1W	nz∙wú÷≪iîL	-
File Items	Bookmarked Items: 0	Spreadsheets:	0	0000	010 5b 06	53 c	b a3 9c f	7 39-23 8	f 7a 69 64 e	4 Of 2c [ .SE£ -	+9# ·zidā ·,	
Total File Items: 4896	Bad Extension: 0	Databases:	0							6 01 ca .N?úÿ -		
Checked Items: 0	Encrypted Files: 0	Graphics:	0							if af eb 1,0\.f		
Unchecked Items: 4896	From E-mail: 0	Multimedia:	0							c 29 01 TÛ"		
Flagged Thumbnails: 0	Deleted Files: 0	E-mail Messages	s: 0							7 88 bf PÙ*;Os		
Other Thumbnails: 0	From Recycle Bin: 0	Executables:	0							e d5 75 i··Þ·ñ f 31 3b ]FIPÓð		
Filtered In: 4896	Duplicate items: 4	Archives:	0							2 19 ad A A 0;		
Filtered Out: 0	OLE Subitems: 0	Folders:	1							0 8d d9 n ú8m#		
Unfiltered Filtered	Flagged Ignore: 0	Slack/Free Space	e: 4895							d 7b 4f "34z -Éû		
All Items Actual Files	KFF Ignorable: 0	Other Known Ty										
Actourt nos	Data Carved Files: 0	Unknown Type:	0	Curse	or position	= 0;	cluster = :	256000; lo	gical sector =	= 256000; physi	cal sector =	
	D 🗳 OFF Unfiltered		All Co	New West		DT	-	- 0				
File Name	Full Path		1111		cycle Bi Ex		- File Type	Category	Subject	Cr Date	Mod Date	
File Name	Full Path	IONAME-Unknown\		Ree		t i				Cr Date	Mod Date	
	Full Path 2nd Image\ (2)//	IONAME-Unknown\\ IONAME-Unknown\\	DriveFreeSp	Rei		t I	File Type	Slack/Free	S			
DriveFreeSpace0001	Full Path 2nd Image\ (2)// 2nd Image\ (2)//		DriveFreeSp DriveFreeSp	Ree a		t I	File Type Drive Free S Drive Free S	Slack/Free	S S	N/A	N/A	
DriveFreeSpace0001	Full Path 2nd Image\ (2)/J 2nd Image\ (2)/J 2nd Image\ (2)/J 2nd Image\ (2)/J	ONAME-Unknown\	DriveFreeSp DriveFreeSp DriveFreeSp	Red a a			File Type Drive Free S Drive Free S Drive Free S	Sladt/Free Sladt/Free	S S	N/A N/A	N/A N/A	
DriveFreeSpace0001 DriveFreeSpace0002 DriveFreeSpace0002 DriveFreeSpace0003 DriveFreeSpace0004 DriveFreeSpace0005	Full Path 2nd Image\ (2)/i 2nd Image\ (2)/i 2nd Image\ (2)/i 2nd Image\ (2)/i 2nd Image\ (2)/i	IONAME-Unknown\ IONAME-Unknown\ IONAME-Unknown\ IONAME-Unknown\	DriveFreeSp DriveFreeSp DriveFreeSp DriveFreeSp DriveFreeSp	Ree a a a a		t	File Type Drive Free S Drive Free S Drive Free S Drive Free S Drive Free S	Slack/Free Slack/Free Slack/Free Slack/Free Slack/Free	S S S S	N/A N/A N/A N/A	N/A N/A N/A N/A	
	Full Path 2nd Image\ (2)/ 2nd Image\ (2)/ 2nd Image\ (2)/ 2nd Image\ (2)/ 2nd Image\ (2)/ 2nd Image\ (2)/	IONAME-Unknown\/ IONAME-Unknown\/ IONAME-Unknown\/ IONAME-Unknown\/ IONAME-Unknown\/	DriveFreeSp DriveFreeSp DriveFreeSp DriveFreeSp DriveFreeSp DriveFreeSp	Ret a a a a			File Type Drive Free S Drive Free S Drive Free S Drive Free S Drive Free S	Slady/Free Slady/Free Slady/Free Slady/Free Slady/Free	S S S S S	N/A N/A N/A N/A N/A	N/A N/A N/A N/A N/A	
	Full Path 2nd Imagei (2)/ 2nd Imagei (2)/	IONAME-Unknown\ IONAME-Unknown\ IONAME-Unknown\ IONAME-Unknown\ IONAME-Unknown\ IONAME-Unknown\ IONAME-Unknown\	DriveFreeSp DriveFreeSp DriveFreeSp DriveFreeSp DriveFreeSp DriveFreeSp DriveFreeSp	Red a a a a a			File Type Drive Free S Drive Free S Drive Free S Drive Free S Drive Free S Drive Free S Drive Free S	SladyFree SladyFree SladyFree SladyFree SladyFree SladyFree SladyFree	S S S S S S S	N/A N/A N/A N/A N/A N/A	N/A N/A N/A N/A N/A N/A	
DriveFreeSpace0001 DriveFreeSpace0002 DriveFreeSpace0002 DriveFreeSpace0005 DriveFreeSpace0005 DriveFreeSpace0005 DriveFreeSpace0005 DriveFreeSpace0005 DriveFreeSpace0005	Full Path 2nd Imagei (2)/ 2nd Imagei (2)/	IONAME-Unknown/ IONAME-Unknown/ IONAME-Unknown/ IONAME-Unknown/ IONAME-Unknown/ IONAME-Unknown/ IONAME-Unknown/	DriveFreeSp DriveFreeSp DriveFreeSp DriveFreeSp DriveFreeSp DriveFreeSp DriveFreeSp DriveFreeSp	Red a a a a a a a			File Type Drive Free S Drive Free S Drive Free S Drive Free S Drive Free S Drive Free S Drive Free S	Slack/Free Slack/Free Slack/Free Slack/Free Slack/Free Slack/Free Slack/Free	S S S S S S S	N/A N/A N/A N/A N/A N/A	N/A N/A N/A N/A N/A N/A N/A	
DriveFreeSpace0001 DriveFreeSpace0002 DriveFreeSpace0002 DriveFreeSpace0003 DriveFreeSpace0005 DriveFreeSpace0005 DriveFreeSpace0007 DriveFreeSpace0007 DriveFreeSpace0007 DriveFreeSpace0007 DriveFreeSpace0009 DriveFreeSpace009	Full Path 2nd Imagei (2)/ 2nd Imagei (2)/	IONAME-Unknown/ IONAME-Unknown/ IONAME-Unknown/ IONAME-Unknown/ IONAME-Unknown/ IONAME-Unknown/ IONAME-Unknown/ IONAME-Unknown/	DriveFreeSp DriveFreeSp DriveFreeSp DriveFreeSp DriveFreeSp DriveFreeSp DriveFreeSp DriveFreeSp	Rei a a a a a a a a.			File Type Drive Free S Drive Free S	Slad/Free Slad/Free Slad/Free Slad/Free Slad/Free Slad/Free Slad/Free Slad/Free	S S S S S S S S	N/A N/A N/A N/A N/A N/A N/A	N/A N/A N/A N/A N/A N/A N/A	
DriveFreeSpace0001 DriveFreeSpace0002 DriveFreeSpace002 DriveFreeSpace004 DriveFreeSpace006 DriveFreeSpace006 DriveFreeSpace006 DriveFreeSpace008 DriveFreeSpace008 DriveFreeSpace008 DriveFreeSpace008 DriveFreeSpace008 DriveFreeSpace008 DriveFreeSpace008 DriveFreeSpace008 DriveFreeSpace008 DriveFreeSpace088 DriveFreeSpace088 DriveFreeSpace088 DriveFreeSpace088 DriveFreeSpace088 DriveFreeSpace888 DriveFreeSpace8888 DriveFreeSpace8888 DriveFreeSpace8888 DriveFreeSpace8888 DriveFreeSpace8888 DriveFreeSpace88888 DriveFreeSpace88888 DriveFreeSpace888888 DriveFreeSpace88888 DriveFreeSpace88888 DriveFreeSpace88888 DriveFreeSpace88888 DriveFreeSpace88888 DriveFreeSpace888888 DriveFreeSpace88888888 DriveFreeSpace888888 DriveFreeSpace888888 DriveFreeSpace888888 DriveFreeSpace88888888 DriveFreeSpace8888888 DriveFreeSpace88888888 DriveFreeSpace888888888 DriveFreeSpace888888 DriveFreeSpace88888 DriveFreeSpace8888888 DriveFreeSpace888888 DriveFreeSpace8888888 DriveFreeSpace88888888 DriveFreeSpace88888888 DriveFreeSpace8888888 DriveFreeSpace8888888 DriveFreeSpace888888 DriveFreeSpace8888888 DriveFreeSpace88888 DriveFreeSpace8888888 DriveFreeSpace88888 DriveFreeSpace88888 DriveFreeSpace88888 DriveFreeSpace88888 DriveFreeSpace88888 DriveFreeSpace88888 DriveFreeSpace88888 DriveFreeSpace88888 DriveFreeSpace88888 DriveFreeSpace8888 DriveFreeSpace8888 DriveFreeSpace8888 DriveFreeSpace8888 DriveFreeSpace888 DriveFr	Full Path           2nd Image(2)0           2nd Image(2)0	IONAME-Unknown/U IONAME-Unknown/U IONAME-Unknown/U IONAME-Unknown/U IONAME-Unknown/U IONAME-Unknown/U IONAME-Unknown/U IONAME-Unknown/U	DriveFreeSp DriveFreeSp DriveFreeSp DriveFreeSp DriveFreeSp DriveFreeSp DriveFreeSp DriveFreeSp DriveFreeSp	Ree a a a a a a a a			File Type Drive Free S Drive Free S	Sladv/Free Sladv/Free Sladv/Free Sladv/Free Sladv/Free Sladv/Free Sladv/Free Sladv/Free Sladv/Free	S S S S S S S S	N/A N/A N/A N/A N/A N/A N/A N/A	N/A N/A N/A N/A N/A N/A N/A N/A N/A	
DriveFreeSpace0001     DriveFreeSpace0002     DriveFreeSpace0002     DriveFreeSpace0005     DriveFreeSpace0005     DriveFreeSpace0007     DriveFreeSpace0007     DriveFreeSpace0007     DriveFreeSpace0009     DriveFreeSpace0009     DriveFreeSpace0009     DriveFreeSpace0019     DriveFreeSpace0019	Full Path 2nd Imagei (2)/ 2nd Imagei (2)/	IONAME-Unknown/ IONAME-Unknown/ IONAME-Unknown/ IONAME-Unknown/ IONAME-Unknown/ IONAME-Unknown/ IONAME-Unknown/ IONAME-Unknown/ IONAME-Unknown/ IONAME-Unknown/	DriveFreeSp DriveFreeSp DriveFreeSp DriveFreeSp DriveFreeSp DriveFreeSp DriveFreeSp DriveFreeSp DriveFreeSp DriveFreeSp DriveFreeSp	Ree a a a a a a a a		t 1	File Type Drive Free S Drive Free S	Sladv/Free Sladv/Free Sladv/Free Sladv/Free Sladv/Free Sladv/Free Sladv/Free Sladv/Free Sladv/Free Sladv/Free	S S S S S S S S	N/A N/A N/A N/A N/A N/A N/A N/A	N/A N/A N/A N/A N/A N/A N/A N/A N/A N/A	
DriveFreeSpace0001 DriveFreeSpace0002 DriveFreeSpace002 DriveFreeSpace004 DriveFreeSpace006 DriveFreeSpace006 DriveFreeSpace006 DriveFreeSpace008 DriveFreeSpace008 DriveFreeSpace008 DriveFreeSpace008 DriveFreeSpace008 DriveFreeSpace008 DriveFreeSpace008 DriveFreeSpace008 DriveFreeSpace008 DriveFreeSpace088 DriveFreeSpace088 DriveFreeSpace088 DriveFreeSpace088 DriveFreeSpace088 DriveFreeSpace888 DriveFreeSpace8888 DriveFreeSpace8888 DriveFreeSpace8888 DriveFreeSpace8888 DriveFreeSpace8888 DriveFreeSpace88888 DriveFreeSpace88888 DriveFreeSpace888888 DriveFreeSpace88888 DriveFreeSpace88888 DriveFreeSpace88888 DriveFreeSpace88888 DriveFreeSpace88888 DriveFreeSpace888888 DriveFreeSpace88888888 DriveFreeSpace888888 DriveFreeSpace888888 DriveFreeSpace888888 DriveFreeSpace88888888 DriveFreeSpace8888888 DriveFreeSpace88888888 DriveFreeSpace888888888 DriveFreeSpace888888 DriveFreeSpace88888 DriveFreeSpace8888888 DriveFreeSpace888888 DriveFreeSpace8888888 DriveFreeSpace88888888 DriveFreeSpace88888888 DriveFreeSpace8888888 DriveFreeSpace8888888 DriveFreeSpace888888 DriveFreeSpace8888888 DriveFreeSpace88888 DriveFreeSpace8888888 DriveFreeSpace88888 DriveFreeSpace88888 DriveFreeSpace88888 DriveFreeSpace88888 DriveFreeSpace88888 DriveFreeSpace88888 DriveFreeSpace88888 DriveFreeSpace88888 DriveFreeSpace88888 DriveFreeSpace8888 DriveFreeSpace8888 DriveFreeSpace8888 DriveFreeSpace8888 DriveFreeSpace888 DriveFr	Full Path 2nd Imagei (2)) 2nd Imagei (2))	IONAME-Unknown/U IONAME-Unknown/U IONAME-Unknown/U IONAME-Unknown/U IONAME-Unknown/U IONAME-Unknown/U IONAME-Unknown/U IONAME-Unknown/U	DriveFreeSp DriveFreeSp DriveFreeSp DriveFreeSp DriveFreeSp DriveFreeSp DriveFreeSp DriveFreeSp DriveFreeSp DriveFreeSp DriveFreeSp	Res a			File Type Drive Free S Drive Free S	Sladv/Free Sladv/Free Sladv/Free Sladv/Free Sladv/Free Sladv/Free Sladv/Free Sladv/Free Sladv/Free	S S S S S S S S	N/A N/A N/A N/A N/A N/A N/A N/A	N/A N/A N/A N/A N/A N/A N/A N/A N/A	

Figure 58. Hex Code of SSD Second Image

**Second image results.** Now in the Search Term box, we search for indexed Words. From the below image we can see a sample number of hits for the search items animals, travel, plant, and sunshine.

	Overview		Explore		Graphics	E-Mail		Sea	arch	
Ir	ndexed Search	Liv	e Search							
-	Search Term:					Add	Imp	ort	Option	ıs
	Indexed Wor	ds	Co	Sea	rch Items			Hits	Files	^
		Indexed Words Co		ani	mal			23	5	
				trav	/el			2	1	T
				pla	nt			5	4	~
				<					>	
				Edi	t Item Remove It	em Remove	All	View Iter	m Result	ts x
				Cumu	lative operator: At		View (	Cumulativ	e Resul	ts

Figure 59. Sample Hits for Animals, Travel, and Plant for SSD Image 2

Overview	Explore	Graphics	E-Mail	Sea	arch	
Indexed Search L Search Term:	ive Search		Add	mport	Option	IS
Indexed Words	tr	earch Items avel lant unshine		Hits 2 5 9	Files 1 4 6	< >
<u></u>	Cun	idit Item Remove It nulative operator: Al	ND OR View	View Iter v Cumulativ		

AccessData FTK 1.81.0 DEMO VERSION -- C:\Users\bharg\Desktop\starred paper\Analysis on 31

Figure 60. Sample Hits for Sunshine, Travel, and Plant for SSD Image 2

Now we search for .doc, .pdf and .xlxs files, and we see the number of hits as follows.

Overview	E	xplore	G	Braphics	E-Mail	Sea	arch
Indexed Search	Live S	Search					
Search Term:					Add	Import	Options
Indexed Wo	rds C	0	Search Ite	ms		Hits	Files
			.doc			1420	1206
			.xlxs			235	228
			Cumulati	ve Results (usi	ng OR)	1655	1371
		1	Edit Item	Remove Item	Remove A	View Iter	m Results
		0	Cumulative o	operator: AND	OR	ew Cumulativ	e Results
*		<u>ها</u> کو		麗 🙆 🖸 🌾	_		

🖟 AccessData FTK 1.81.0 DEMO VERSION -- C:\Users\bharg\Desktop\starred paper\Analysis or

Figure 61. Sample Hits for .Doc and .Xlxs for SSD Image 2

	ools Help						
Overview	Explore	G	raphics	E-Mail	568	arch	
Indexed Search Li	ve Search						
Search Term:				Add	mport	Option	s
Indexed Words	Co	Search Ite	ms		Hits	Files	^
		.doc			1420	1206	
		.xlxs			235	228	
		.pdf			4519	1441	¥
		<				>	
		Edit Item	Remove Ite	em Remove All	View Iter	n Result	s »
		Cumulative o	perator: AN	ND OR View	v Cumulativ	e Result	s»
				D			_
, m	୍ 🕷 🖂	) 🐺 🚟 i	r 🙆 🙆	(# T			

AccessData FTK 1.81.0 DEMO VERSION -- C:\Users\bharg\Desktop\starred paper\Analysis on

Figure 62. Sample Hits for .Doc, .Pdf, and .Xlxs for SSD Image 2

Now we fill in the case information such as Case Number, Case Name, Case Path, and Case Folder and click on next.

Analysis of SSD third image.

Forensir		AccessData's Forensic Toolkit®-FTK® The Complete Analysis Tool	D
Text Compare Contents Contract and Contents		Wizard for Creating a New Cas	se
nvestigator Name: 🚦	hargav	~	
Case Information			
	Case Number:	003	
	Case Name:	Analysis on 3rd Image Acquired from SSD	
	Case Path:	C:\Users\bharg\Desktop\starred paper\	Browse
Case Description:	Case Folder:	C:\Users\bharg\Desktop\starred paper\Analysis on 3rd	d Image Acqui
			1
			_

Figure 63. Creating a New Case for SSD Image 3

Now we fill the evidence information, such as Evidence location, Evidence Display

Name and click on OK.

Evidence Information	×
Evidence Location:	
C:\Images\SSD Images\3rd Image.ad1	
Evidence Display Name:	
3rd Image	
Evidence Identification Name/Number:	
Comment:	
Local Evidence Time Zone:	
Eastern Time with Daylight Saving (US - New	/ York) 🗸 🗸
ОК	Cancel

*Figure 64*. Evidence Information for SSD Third Image

Now we see the status of the image analysis.

\lmages\SSD	lmages\3rd lmage.ad1		
rrent File Item	:		
'd Image\ (2)\N	IONAME-Unknown\DriveFreeSpace	:0005	
Current File Ite	m Status	Total Process Status	
Action:	Filtering Text	Elapsed Time:	0.00:00:10
File	Drive Free Space	Total Items Examined:	18
Item	26,214,400 (5 of 4877)	Total Items Added:	18
Progress:	22,833,956	Total Items Indexed:	6

Figure 65. Leaving Time Zone when Processing an Image 2

Results of SSD third image. After the image analysis is done, we can see the number of

files. When we click on one of the files, we can see the Hex code format as follows:

	Help																
Overview Exp	lore	Graphics	E-Mail	Searc	h i	Bookmark											
Evidence Items	File	Status	File Categor	ry	<u>*</u>	~ *	70 🚔 🔛 H	6 6	1 🔊								
vidence Items: 3	KFF Alert File	es: 0	Documents:	0			a constant										
File Items	Bookmarked	Items: 0	Spreadsheets:	0			5 58 46 41 54 0 00 00 00 00				EV EXFAT		-				
otal File Items: 4896	Bad Extensi	on: O	Databases:	0									2				
hecked items: 0	Encrypted F	iles: 0	Graphics:	0			0 00 00 00 00										
Inchecked Items: 4896	From E-mail:	0	Multimedia:	0	0000040	00 48 06 00	0 00 00 00 00	-00 78	el 0e 00 0	00 00 00	H	xá · · · ·	2				
lagged Thumbnails: 0	Deleted Files	. 0	E-mail Messages:	0			0 00 le 00 00										
Other Thumbnails: 0			Executables:	0			31 8c c6 d6				····1 · EÖ ·						
iltered In: 4896			Archives:	0			0 00 00 00 00 1 00 7c 88 16										
itered Out: 0			Folders:	1			1 00 7C 88 10 1 fb 55 aa 75										
Unfiltered Filtered	Flagged Igno		Slack/Free Space:	4895			b0 65 e8 a6										
All tems Actual Files			Other Known Type														
All Lenis Actual Files	Data Carved			0	Cursor po	sition = 0: c	luster = 0; lo	nical se	ctor = 0: pl	vsical se	ctor = 411	648					
8 88 🚳 🎨 🖪		F Unfiltered		All Col		~ D12											
Ext File Type	Category	Subject	∨ ∏ Cr Date	Mod	d Date	Acc Dat		-Size	P-Size	Children	Descen		Del Rec	cyc C		Sector	
. Ext File Type Root Folder	Category Folder		Cr Date N/A	Moo N/A	d Date	Acc Dat		512	2 51	2 12	12		Del Rec	cyc C	Full	6,374	
. Ext File Type Root Folder File system	Category Folder Stad/Free S		Cr Date N/A N/A	Moc N/A N/A	d Date	Acc Dat N/A N/A		612 612	2 51 2 51	2 12 2 0	12		Del Rec	cyc C	Full Full	6,374 250,069,6	
. Ext File Type Root Folder File system File system	Category Folder Slack/Free S. Slack/Free S.		Cr Date N/A N/A N/A	Moo N/A N/A N/A	d Date	Acc Dat N/A N/A N/A	e L	512 512 16,384	2 51 2 51 10,38	2 12 2 0 4 0	2 12 0 0		Del Red	cyc C	Full Full	6,374	
Ext File Type Root Folder File system File system Drive Free S	Category Folder Slad/Free S. Slad/Free S. Slad/Free S.		Cr Date N/A N/A N/A	Moo N/A N/A N/A	d Date	Acc Dat N/A N/A N/A N/A	e L	512 512 18,384 26,214,400	2 51 2 51 18,38 127,824,5	2 12 2 0 4 0	2 12 0 0		Del Red	cyc C	Full Full Full Full	6,374 250,069,6	
Ext File Type Root Folder File system File system	Category Folder Slad/Free S. Slad/Free S. Slad/Free S. Slad/Free S.		Cr Date N/A N/A N/A	Moo N/A N/A N/A	d Date	Acc Dat N/A N/A N/A	e L	512 512 16,384	2 51 2 51 16,38 127,824,5 0 127,824,5	2 12 2 0 4 0 0	12 0 0 0 0 0 0		Del Rec	sye C	Full Full	6,374 250,069,6	
. Ext File Type Root Folder File system File system Drive Free S Drive Free S	Category Folder Slad:/Free S. Slad:/Free S. Slad:/Free S. Slad:/Free S.		Cr Date N/A N/A N/A N/A N/A	Moo N/A N/A N/A N/A	d Date	Acc Dat N/A N/A N/A N/A	e L	512 512 16,384 26,214,400 26,214,400	2 51 2 51 10,38 0 127,824,5 0 127,824,5 0 127,824,5	2 12 2 0 4 0 0 0			Del Red	:yc C	Full Full Full Full	6,374 250,069,6	
Ext File Type Root Folder File system File system Drive Free S Drive Free S Drive Free S	Category Folder Slad:/Free S. Slad:/Free S. Slad:/Free S. Slad:/Free S. Slad:/Free S.		Cr Date N/A N/A N/A N/A N/A N/A	Moo N/A N/A N/A N/A N/A	d Date	Acc Dat N/A N/A N/A N/A N/A	e L	612 512 16,384 26,214,400 26,214,400 26,214,400	2 51 2 51 10,38 0 127,824,5 0 127,824,5 0 127,824,5 0 127,824,5	2 12 2 0 4 0 0 0			Del Red	cyc C	Full Full Full Full Full	6,374 250,069,6	
Ext File Type Root Folder File system File system Drive Free S Drive Free S Drive Free S	Category Folder Sladk/Free S. Sladk/Free S. Sladk/Free S. Sladk/Free S. Sladk/Free S. Sladk/Free S.	Subject	Cr Date N/A N/A N/A N/A N/A N/A N/A	Moo N/A N/A N/A N/A N/A N/A	d Date	Acc Dat N/A N/A N/A N/A N/A N/A	e L	512 512 16,384 26,214,400 26,214,400 26,214,400 26,214,400	2 51 2 51 4 16,38 0 127,824,5 0 127,824,5 0 127,824,5 0 127,824,5 0 127,824,5 0 127,824,5	2 12 2 0 4 0 0 0 0			Del Rec	cyc C	Full Full Full Full Full Full	6,374 250,069,6	
Ext         File Type Root Folder           File system         File system           Drive Free S         Drive Free S           Drive Free S         Drive Free S           Drive Free S         Drive Free S	Category Folder SladvFree S SladvFree S SladvFree S SladvFree S SladvFree S SladvFree S SladvFree S	Subject	Cr Date N/A N/A N/A N/A N/A N/A N/A N/A	Moo N/A N/A N/A N/A N/A N/A	d Date	Acc Dat N/A N/A N/A N/A N/A N/A N/A N/A	e L	512 512 16,384 26,214,400 26,214,400 26,214,400 26,214,400 26,214,400	2 511 2 511 10,38 0 127,824,5 0 127,824,5 0 127,824,5 0 127,824,5 0 127,824,5 0 127,824,5 0 127,824,5 0 127,824,5	2 12 2 0 4 0 0 0 0 0 0			Del Rec	cyc C	Full Full Full Full Full Full Full	6,374 250,069,6	
Fat         File Type           Root Folder         File system           File system         File system           Drive Free S         Drive Free S           Drive Free S         Drive Free S	Category Folder Sladk/Free S. Sladk/Free S. Sladk/Free S. Sladk/Free S. Sladk/Free S. Sladk/Free S. Sladk/Free S. Sladk/Free S.	Subject	Cr Date N/A N/A N/A N/A N/A N/A N/A N/A N/A N/A	Moo N/A N/A N/A N/A N/A N/A N/A N/A	d Date	Acc Dat N/A N/A N/A N/A N/A N/A N/A N/A N/A N/A	e L	512 512 16,384 26,214,400 26,214,400 26,214,400 26,214,400 28,214,400 28,214,400 28,214,400 28,214,400	2 51 2 51 16.38 127.824.5 127.824.5 127.824.5 127.824.5 127.824.5 127.824.5 127.824.5 127.824.5 127.824.5 127.824.5 127.824.5 127.824.5	2 12 2 0 4 0 0 0 0 0 0 0			Del Rea	cyc C	Full Full Full Full Full Full Full Full	6,374 250,069,6	
Ext         File Type           Root Folder         File system           File system         File system           Drive Free S         Drive Free S           Drive Free S         Drive Free S	Category Folder Sladv/Free S Sladv/Free S Sladv/Free S Sladv/Free S Sladv/Free S Sladv/Free S Sladv/Free S Sladv/Free S Sladv/Free S	Subject	Cr Date N/A N/A N/A N/A N/A N/A N/A N/A N/A N/A	Mot           N/A	d Date	Acc Dat           N/A	e L	512 512 18,384 28,214,400 20,214,400 26,214,400 26,214,400 26,214,400 26,214,400 26,214,400 26,214,400 26,214,400	2 51 2 51 10,39 127,824,5 127	2 12 2 0 4 0 0 0 0 0 0 0			Del Red	cyc C	Full Full Full Full Full Full Full Full	6,374 250,069,6	
File Type Root Folder File system File system Drive Free S Drive Free S	Category Folder SladvFree S SladvFree S SladvFree S SladvFree S SladvFree S SladvFree S SladvFree S SladvFree S SladvFree S SladvFree S	Subject	Сг Date N/A N/A N/A N/A N/A N/A N/A N/A N/A N/A	Mot           N/A	d Date	Acc Dat           N/A	e L	512 512 18,384 28,214,400 28,214,400 28,214,400 28,214,400 28,214,400 28,214,400 28,214,400 28,214,400 28,214,400	2 51 2 51 10.38 127,824,5 127	2 12 2 0 4 0 0 0 0 0 0 0 0 0 0 0			Del Rec	cyc C	Full Full Full Full Full Full Full Full	6,374 250,069,6	
Ext File Type Root Folder File system - File system - Drive Free S. Drive Free S.	Category Folder SladvFree S SladvFree S	Subject	Сг Date N/A N/A N/A N/A N/A N/A N/A N/A N/A N/A	Mot           N/A           N/A	d Date	Acc Dat           N/A           N/A	e L	512 512 18,384 26,214,400 28,214,400 28,214,400 28,214,400 28,214,400 28,214,400 28,214,400 28,214,400 28,214,400 28,214,400	2 51 2 51 2 51 10.38 127.824.5 127.824.	2 12 2 0 4 0 0 0 0 0 0 0 0 0 0			Del Rec	tyc C	Full Full Full Full Full Full Full Full	6,374 250,069,6	
File Type           Root Folder           File system           File system           Drive Free S.	Category Folder SladvFree S SladvFree S	Subject	Сг Date N/A N/A N/A N/A N/A N/A N/A N/A N/A N/A	Mot           N/A	d Date	Acc Dat           N/A	e L	512 512 18,384 28,214,400 28,214,400 28,214,400 28,214,400 28,214,400 28,214,400 28,214,400 28,214,400 28,214,400	2 51 2 51 4 16.38 127.824.5 1	2 12 2 0 4 0 			Del Rec	tyc C	Full Full Full Full Full Full Full Full	6,374 250,069,6	

Thes. When we ence on one of the mes, we can see the mex code format as follow

Figure 66. Hex Code for SSD Third Image

Now in the Search Term box, we search for indexed Words. From the below image we

can see a sample number of hits for the search items animals, travel, plant, and sunshine.

e Edit View T	ools He	p				
Overview	Explore	Graphics	E-Mail	Se	arch	
Indexed Search L	ive Search					
Search Term: food	1 25	L A	Add Im	port	Option	ns
Indexed Words	Co ^	Search Items		Hits	Files	1
food	174	animals		12	6	
food0	1	plant		1	1	
food0h	2	travel		0	0	~
food3	1	<			>	
food3yp	1	Edit Item Remove Item	Remove All	View Iter	m Resul	ts

Figure 67. Sample Hits for Animals, Travel, and Plant for SSD Image 3

Overview	Explore	Graphics	E-Mail	Se	arch	
In List by file nan	ne ve Search					
Search Term:			Add	Import	Optior	ıs
Indexed Word	ls Co	Search Items		Hits	Files	^
		plant		1	1	
		travel		0	0	
		sunshine		6	4	~
		<			>	
		Edit Item Remove	e Item Remove Al	View Ite	m Result	s ı
		Cumulative operator:	AND OR Vi	ew Cumulati		te i

Figure 68. Sample Hits for Sunshine, Travel, and Plant for SSD Image 3

Now we search for .doc, .pdf and .xlxs files, and we see the number of hits as follows.

Overview	Explore		Graphics	E-Mail		Sea	irch
Indexed Search	Live Search		orupinea	L-mui			
Search Term:				Add	Impo	rt	Options
Indexed Word	ls Co	Search	Items			Hits	Files
		.doc				1245	1073
		.xlxs				260	245
		Cumu	lative Results (u	ising OR)		1505	1254
		Edit Ite	em Remove It	em Remove	<b>All</b> Vi	ew Iten	n Results a
		Cumulati	ve operator: Al	ND OR	/iew Cu	mulativ	e Results :
animal	<b>N</b>	<u> </u>	क्षे सिंही 🤒 횐				

Figure 69. Sample Hits for .Doc and .Xlxs for SSD Image 3

ile Edit View	Tools	нер					
Overview	Expl	ore	Graphics	E-Mail	Se	arch	
Indexed Search	Live Sea	rch					
Search Term:				Add	Import	Option	ıs
Indexed Wor	rds Co	Sea	irch Items		Hits	Files	1
		.do	c		1245	1073	
		.xbx	s		260	245	I
		pd	F		1971	1310	•
		<				>	
		Ec	it Item Remove I	tem Remove A	View Ite	m Result	s
		Cum	lative operator: A	ND OR V	iew Cumulati	ve Resul	ts
							_

🖟 AccessData FTK 1.81.0 DEMO VERSION -- C:\Users\bharg\Desktop\starred paper\Analysis o

Figure 70. Sample Hits for .Doc, .Pdf, and .Xlxs for SSD Image 3

Analysis of SSD fourth image. Now we fill in the case information such as Case

Number, Case Name, Case Path, and Case Folder and click on next.

Forensic		AccessData's Forensic Toolkit®-FTK The Complete Analysis Too	-
Toolkit		Wizard for Creating a New Ca	ase
nvestigator Name: 🖪	hargav	~	
Case Information			1
	Case Number:	004	
	Case Name:	Analysis on 4th image Acquired from SSD	]
	Case Path:	C:\Users\bharg\Desktop\starred paper\	Browse
Case Description:	Case Folder:	C:\Users\bharg\Desktop\starred paper\Analysis on 4	th image Acquir
			~

Figure 71. Creating a New Case for SSD Image 4

Now we fill the evidence information, such as Evidence location, Evidence Display

Name and click on OK.

	es\4th Image.	ad1	
Evidence Display Na	ne:		
4th Image			
Evidence Identificatio	n Name/Numl	ber:	
004			
Comment:			
Local Evidence Time	Zone:		

*Figure 72.* Evidence Information for SSD Image 4

Now we see the status of the image analysis.

c.filliagestssp.i	mages\4th Image.ad1		
Current File Item	:		
4th Image\ (2)\N	ONAME-Unknown\DriveFreeSpac	e0003	
Current File Iter	n Status	Total Process Status	
Action:	Filtering Text	Elapsed Time:	0.00:00:13
File	Drive Free Space	Total Items Examined:	16
Item	26,214,400 (3 of 4877)	Total Items Added:	16
		Total Items Indexed:	4

Figure 73. Leaving Time Zone when Processing an Image 4

After the image analysis is done, we can see the number of files. When we click on one

of the files, we can see the Hex code format as follows:

Edit Vie	ew Tools I	Help														
Overview	Explo	ore G	Graphics	E-Mail	Search	Bookmark										
Evidence	ce Items	File S	tatus	File Cate	gory #	1 J A	<b>७२ 🚔 🔛 🙀 </b> 🗹	#1								
Evidence Item	ms: 3	KFF Alert File	s: 0	Documents:	•	r 104		2								_
File It	Items	Bookmarked I	Items: 0	Spreadsheets:	0											
otal File Items	ns: 4896	Bad Extension	n: 0	Databases:	0											
hecked Item	ns: 0	Encrypted File	es: 0	Graphics:	0											
nchecked Ite	tems: 4896	From E-mail:	0	Multimedia:	0											
lagged Thum	mbnails: 0	Deleted Files:	0	E-mail Message	s: 0											
ther Thumbr	nails: 0	From Recycle	e Bin: 0	Executables:	0											
iltered In:	4896	Duplicate Item	ns: 4	Archives:	0											
iltered Out:	0	OLE Subitems	s: 0	Folders:	1											
Unfiltered	Filtered	Flagged Ignor	re: 0	Slack/Free Spa	ce: 4895											
All Items	Actual Files	KFF Ignorable	e: 0	Other Known T	ype: 0											
		Data Carved	Files: 0	Unknown Type:	0 <											
	ile Type	•	Unfiltered Subject	∽ Cr Date	All Column Mod Da		L-Size	P-Size	Children	Descen I	Enc D	el Recyc	Crv	ldx	Sector	
		Category					L-Size	P-Size	Children	Descen I	Enc D	el Recyc	Crv	ldx	Sector	
Ext Fi	File Type toot Folder	Category Folder		Cr Date N/A	Mod Da N/A	te Acc Date	512	512	12	12	Enc D	el Recyc	Crv	Full	6,37	
. Ext Fi Ro Fil	file Type toot Folder file system	Category Folder Slad/Free S		Cr Date N/A N/A	Mod Da N/A N/A	te Acc Date N/A N/A	512 512	512 512	12 0	12 0	Enc D	el Recyc	Crv	Full	6,37 250,069	0
Ext Fi	file Type toot Folder file system file system	Category Folder Sladk/Free S Sladk/Free S		Cr Date N/A N/A N/A	N/A N/A N/A	nte Acc Date N/A N/A N/A	512 512 10,384	512 512 16,384	12 0 0	12 0 0	Enc D	el Recyc	Crv	Full Full Full	6,37	
Ext Fi Ro Fil Dr	File Type Root Folder Folder File system Prive Free S	Category Folder Sladk/Free S Sladk/Free S Sladk/Free S		Cr Date N/A N/A N/A N/A	Mod Da N/A N/A N/A N/A	tte Acc Date N/A N/A N/A N/A	512 512 16,384 26,214,400	512 512 16,384 127,824,5	12 0 0	12 0 0	Enc D	el Recyc	Crv	Full Full Full	6,37 250,069	0
Ext Fi Ro Fil Dri Dri	File Type Root Folder file system frive Free S krive Free S	Category Folder Sladk/Free S Sladk/Free S Sladk/Free S Sladk/Free S		Cr Date N/A N/A N/A N/A N/A	Mod Da N/A N/A N/A N/A N/A	te Acc Date N/A N/A N/A N/A N/A	512 512 18,384 26,214,400 26,214,400	512 512 18,384 127,824,5 127,824,5	12 0 0 0	12 0 0 0	Enc D	el Recyc	Crv	Full Full Full Full	6,37 250,069	
. Ext Fi Re Fil Dr Dr Dr	File Type toot Folder ile system irive System trive Free S trive Free S	Category Folder Sladv/Free S Sladv/Free S Sladv/Free S Sladv/Free S		Cr Date N/A N/A N/A N/A	Mod Da N/A N/A N/A N/A	tte Acc Date N/A N/A N/A N/A	512 512 18,384 26,214,400 26,214,400 26,214,400	512 512 10,384 127,824,5 127,824,5 127,824,5	12 0 0	12 0 0	Enc D	el Recyc	Crv	Full Full Full	6,37 250,069	
Ext File	File Type toot Folder ile system irive Free S trive Free S trive Free S trive Free S	Category Folder Sladv/Free S Sladv/Free S Sladv/Free S Sladv/Free S		Cr Date N/A N/A N/A N/A N/A N/A	Mod Da N/A N/A N/A N/A N/A N/A	te Acc Date N/A N/A N/A N/A N/A N/A	512 512 18,384 26,214,400 26,214,400	512 512 10,384 127,824,5 127,824,5 127,824,5 127,824,5	12 0 0 0 0 0	12 0 0 0 0	Enc D	el Recyc	Crv	Full Full Full Full Full Full	6,37 250,069	0
Ext Fi	File Type toot Folder ile system irive Free S trive Free S trive Free S trive Free S	Category Folder Sladk/Free S Sladk/Free S Sladk/Free S Sladk/Free S Sladk/Free S		Cr Date N/A N/A N/A N/A N/A N/A N/A	Mod Da N/A N/A N/A N/A N/A N/A N/A	ke Acc Date N/A N/A N/A N/A N/A N/A	512 512 10.384 26.214.400 26.214.400 26.214.400 26.214.400	512 512 10,384 127,824,5 127,824,5 127,824,5 127,824,5 127,824,5	12 0 0 0 0 0 0	12 0 0 0 0 0 0	Enc D	el Recyc	Crv	Full Full Full Full Full Full	6,37 250,069	),e
. Ext Fi Re Fill Dr Dr Dr Dr Dr Dr	File Type toot Folder ile system ile system trive Free S trive Free S trive Free S trive Free S	Category Folder SladvFree S SladvFree S SladvFree S SladvFree S SladvFree S SladvFree S SladvFree S		Cr Date N/A N/A N/A N/A N/A N/A N/A N/A	Mod Da N/A N/A N/A N/A N/A N/A N/A N/A	te Acc Date N/A N/A N/A N/A N/A N/A N/A	512 512 18,384 28,214,400 28,214,400 28,214,400 28,214,400 28,214,400	512 512 18,384 127,824,5 127,824,5 127,824,5 127,824,5 127,824,5 127,824,5	12 0 0 0 0 0 0 0	12 0 0 0 0 0 0 0	Enc D	el Recyc	Crv	Full Full Full Full Full Full Full	6,37 250,069	),e
Ext Fill Fill Dr Dr Dr Dr Dr Dr Dr Dr Dr Dr	File Type toot Folder ile system ile system trive Free S trive Free S trive Free S trive Free S trive Free S trive Free S	Category Folder Sladd/Free S Sladd/Free S Sladd/Free S Sladd/Free S Sladd/Free S Sladd/Free S Sladd/Free S Sladd/Free S		Cr Date N/A N/A N/A N/A N/A N/A N/A N/A N/A	Mod Da N/A N/A N/A N/A N/A N/A N/A N/A N/A N/A	te Acc Date N/A N/A N/A N/A N/A N/A N/A N/A N/A N/A	512 512 16,384 26,214,400 26,214,400 26,214,400 26,214,400 26,214,400 26,214,400 26,214,400 26,214,400	512 512 10,384 127,824,5 127,824,5 127,824,5 127,824,5 127,824,5 127,824,5 127,824,5	12 0 0 0 0 0 0 0 0 0 0 0	12 0 0 0 0 0 0 0 0 0 0 0 0	Enc D	el Recyc	Crv	Full Full Full Full Full Full Full Full	6,37 250,069	
Ext Fi Rc Fil Dr Dr Dr Dr Dr Dr Dr Dr Dr Dr Dr	Tile Type loot Folder ile system ile system irive Free S trive Free S	Category Folder Sladd/Free S Sladd/Free S Sladd/Free S Sladd/Free S Sladd/Free S Sladd/Free S Sladd/Free S Sladd/Free S		Cr Date N/A N/A N/A N/A N/A N/A N/A N/A N/A N/A	Mod Da           N/A	tte Acc Date N/A N/A N/A N/A N/A N/A N/A N/A N/A N/A	512 512 10.384 26.214.400 26.214.400 26.214.400 26.214.400 26.214.400 26.214.400 26.214.400 26.214.400 26.214.400	512 512 10,384 127,824,5 127,824,5 127,824,5 127,824,5 127,824,5 127,824,5 127,824,5 127,824,5	12 0 0 0 0 0 0 0 0 0 0 0 0 0	12 0 0 0 0 0 0 0 0 0 0 0 0 0	Enc D	el Recyc	Crv	Full Full Full Full Full Full Full Full	6,37 250,069	
Ext Fi	Tile Type loot Folder ile system ile system trive Free S trive Free S	Category Folder Sladd/Free S Sladd/Free S Sladd/Free S Sladd/Free S Sladd/Free S Sladd/Free S Sladd/Free S Sladd/Free S Sladd/Free S Sladd/Free S		Cr Date N/A N/A N/A N/A N/A N/A N/A N/A N/A N/A	Mod Da           N/A	te Acc Date N/A N/A N/A N/A N/A N/A N/A N/A N/A N/A	512 512 10.384 26.214,400 26.214,400 26.214,400 26.214,400 26.214,400 26.214,400 26.214,400 26.214,400 26.214,400	512 512 10,384 127,824,5 127,824,5 127,824,5 127,824,5 127,824,5 127,824,5 127,824,5 127,824,5 127,824,5	12 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	12 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	Enc D	el Recyc	Crv	Full Full Full Full Full Full Full Full	6,37 250,069	
Ext Fi Fill Fill Dr Dr Dr Dr Dr Dr Dr Dr Dr Dr Dr Dr Dr	Tile Type loot Folder ile system ile system ile system S trive Free S	Category Folder Sladv/Free S Sladv/Free S		Cr Date N/A N/A N/A N/A N/A N/A N/A N/A N/A N/A	Mod Da           N/A	te Acc Date NA NA NA NA NA NA NA NA NA NA NA NA NA	512 613 26,214,400 26,214,400 26,214,400 26,214,400 26,214,400 26,214,400 26,214,400 26,214,400 26,214,400 26,214,400 26,214,400	512 512 16,384 127,824,5 127,824,5 127,824,5 127,824,5 127,824,5 127,824,5 127,824,5 127,824,5 127,824,5 127,824,5	12 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	12 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	Enc D	el Recyc	Crv	Full Full Full Full Full Full Full Full	6,37 250,069	0
Ext Fi	The Type loot Folder ile system ile system ile system S trive Free S	Category Folder Sladk/Free S Sladk/Free S Sladk/Free S Sladk/Free S Sladk/Free S Sladk/Free S Sladk/Free S Sladk/Free S Sladk/Free S Sladk/Free S		Cr Date N/A N/A N/A N/A N/A N/A N/A N/A N/A N/A	Mod Da           N/A           N/A	te Acc Date NA NA NA NA NA NA NA NA NA NA NA NA NA	512 512 10.384 26.214.400 26.214.400 26.214.400 26.214.400 26.214.400 26.214.400 26.214.400 26.214.400 26.214.400 26.214.400	512 512 16,384 127,824,5 127,824,5 127,824,5 127,824,5 127,824,5 127,824,5 127,824,5 127,824,5 127,824,5 127,824,5 127,824,5	12 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	12 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	Enc D	el Recyc	Crv	Full Full Full Full Full Full Full Full	6,37 250,069	
Ext Fill Fill Fill Fill Fill Fill Fill Fill	Tile Type loot Folder ile system ile system ile system S trive Free S	Category Folder SladkFree S SladkFree S		Cr Date N/A N/A N/A N/A N/A N/A N/A N/A N/A N/A	Mod Da           N/A	te Acc Date NA NA NA NA NA NA NA NA NA NA NA NA NA	512 612 10.384 26.214.400 26.214.400 26.214.400 26.214.400 26.214.400 26.214.400 26.214.400 26.214.400 26.214.400 26.214.400 26.214.400 26.214.400	512 512 16,384 127,824,5 127,824,5 127,824,5 127,824,5 127,824,5 127,824,5 127,824,5 127,824,5 127,824,5 127,824,5	12 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	12 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	Enc D	el Recyc	Crv	Full Full Full Full Full Full Full Full	6,37 250,069	

Figure 74. Hex Code for SSD Fourth Image

Now in the Search Term box, we search for indexed Words. From the below image we can see a sample number of hits as 0 for the search items animals, travel, plant, and sunshine.

ile E	dit View	Tools	Hel	р							
Ov	erview	E	kplore		Graphics		E-Mail		Sea	arch	
Inde	xed Search	Live S	earch								
Sea	arch Term:						Add	Im	nport	Optior	ıs
In	dexed Wor	ds Co	0	Sea	rch Items				Hits	Files	^
				ani	mal				0	0	
				pla	nt				0	0	П
				trav	/el				0	0	¥
				<						>	
				Ed	it Item Remove	e Item	Remove	All	View Iter	m Result	ts »
				Cumu	lative operator:	AND	OR	View	Cumulativ	e Resul	ts »
<u>, m</u>		~ 4	بر   †	9 ≙	। 📅 🕅 😣	2) 🐔					

AccessData FTK 1.81.0 DEMO VERSION -- C:\Users\bharg\Desktop\starred paper\Analysis o

Figure 75. Sample Hits for Animals, Travel, and Plant for SSD Image 4

Overview	Explore	e	Graphics	E-Mail	Se	arch	
Indexed Search	Live Searc	h					
Search Term:				Add	Import	Option	ns
Indexed Wo	rds Co	Search	Items		Hits	Files	^
		plant			0	0	
		travel			0	0	
		sunshi	ne		0	0	¥
		<				>	
		Edit Ite	m Remove It	em Remove All	View Ite	m Result	ts »
		Cumulativ	e operator: Al	VD OR Vie	w Cumulati	ve Resu	ts »

AccessData FTK 1.81.0 DEMO VERSION -- C:\Users\bharg\Desktop\starred paper\Analysis on

Figure 76. Sample Hits for Sunshine, Travel, and Plant for SSD Image 4

Now we search for .doc, .pdf and .xlxs files, and we see the number of hits as 0, and we can see as follows.

	Em	-	Orachian	E Mail		Sec	arch	
view	EX	piore	Graphics	E-Mail		366	arch	
d Search	Live Se	arch						
h Term:				Add	Imp	ort	Option	IS
exed Word	ls Co		Search Items			Hits	Files	^
			.pdf			0	0	
			.doc			0	0	Т
			.xlxs			0	0	~
			<				>	
			Edit Item Remove	e Item Remove	All	View Iter	n Result	is »
			Cumulative operator:	AND OR	View (	Cumulativ	e Resul	ts x
	h Term:	d Search Live Se	d Search Live Search h Term: exed Words Co	d Search Live Search h Term: exed Words Co Search Items .pdf .doc .xlxs < Edit Item Remove	d Search Live Search h Term: Add exed Words Co .pdf .doc .xbxs < Edit Item Remove Item Remove	d Search Live Search h Term: Add Imp exed Words Co .pdf .doc .xlxs < Edit Item Remove Item Remove All	d Search Live Search h Term: Add Import exed Words Co Search Items .pdf 0 .doc 0 .xlxs 0 < Edit Item Remove Item Remove All View Iter	d Search Live Search h Term: Add Import Option exed Words Co Search Items Hits Files .pdf 0 0 .doc 0 0 .xlxs 0 0 < Edit Item Remove Item Remove All View Item Result

🔏 AccessData FTK 1.81.0 DEMO VERSION -- C:\Users\bharg\Desktop\starred paper\Analysis c

Figure 77. Sample Hits for .Doc, .Pdf, and .Xlxs for SSD Image 4

Now when we search for a specific item (animal), we get the hits as 0 which is far less

than the results obtained from previous images.

AccessData FTK 1.81.0 DEMO VERSION -- C:\Users\bharg\Desktop\starred paper\Analysis on

Overview		Explor		Graphics	E-Mail		Sea	arch
Ir List by boo	okmark n	ame arc	:h					
Search Terr	n:				Add	Im	port	Options
Indexed	Words	Co	Sea	rch Items			Hits	Files
			ani	mal			0	0
				it Item Remove It				m Results
			Cumu	lative operator: Al	ND OR	View	Cumulativ	re Results

Figure 78. Sample Hits for Animals, Travel, and Plant for SSD Image 4

Words. From the below image we can see a sample number of hits for the search items animals, travel, plant, and sunshine.

Results obtained from HDD. Now in the Search Term box, we search for indexed

Overview	Explore	(	Graphics	E-Mail		Sea	arch	
Indexed Search	Live Search							
Search Term:				Add	Imp	ort	Option	ıs
Indexed Word	ls Co	Search Ite	ems			Hits	Files	1
		animal				1676	39	
		plant				1147	11	I
		travel				2053	55	•
		<					>	
		Edit Item	Remove It	em Remove	All	/iew Iter	n Result	S
		Cumulative	operator: A	ND OR	View (	umulativ	e Resul	ts

Figure 79. Sample Hits for Animals, Travel, and Plant for HDD Image

AccessData FTK 1.81.0 DEMO VERSION -- C:\Users\bharg\Desktop\starred paper\Analysis on File Edit View Tools Help

Overview	Explore	Graphics	E-Ma	ul	Sea	arch	
Indexed Search	Live Search						
Search Term:			Add	Im	port	Option	ıs
Indexed Word	ls Co	Search Items			Hits	Files	^
		plant			1147	11	
		travel			2053	55	
		sunshine			808	4	¥
		<				>	
		Edit Item Remo	ve Item Remo	ve All	View Iter	n Result	s »
	Ci	umulative operator:	AND OR	View	Cumulativ	e Resul	ts »
		<u> </u>					
<u></u>	~ 🐺 ро	😽 🖼 🔂	O] 🐔				

Figure 80. Sample Hits for Sunshine, Travel, and Plant for HDD Image

Now we search for .doc, .pdf and .xlxs files, and we see the number of hits as 0, and we

can see as follows.

AccessData FTK 1.81.0 DEMO VERSION -- C:\Users\bharg\Desktop\starred paper\Analysis o
 File Edit View Tools Help

Overview	Explore	G	Graphics	E-Mail		Sea	arch	
Indexed Search	Live Search							
Search Term:				Add	Imp	ort	Option	s
Indexed Word	ds Co	Search Ite	ems			Hits	Files	1
		.pdf				2688	102	
		.xlxs				5	5	I
		.doc				3716	182	•
		<					>	
		Edit Item	Remove Ite	Remove	All	View Iter	n Result	s :
		Cumulative of	operator: AN	D OR	View C	Cumulativ	e Resul	s
				_				
<u>_</u> M	~ 🐴 🕞	ə 🚔 🔛 i	📸 🥺 횐	<b>e</b> 1				

Figure 81. Sample Hits for .Doc, .Pdf, and .Xlxs for HDD Image

When we analyze the Hard Disk Drive using FTK, we can see the total number of files as

of 5000.

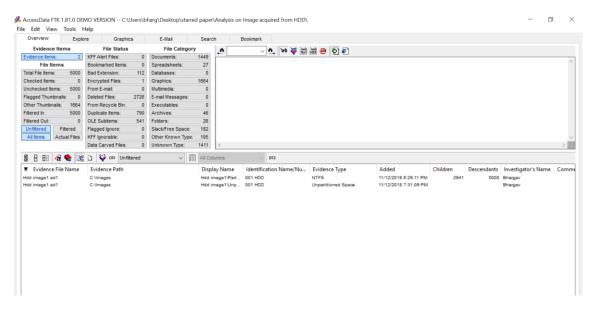


Figure 82. Total Number of Files Generated for HDD Image

When we click on one of the image files, we can recover it, and we can see the preview

## of the images as follows.

Overview E:	xplor	e Graphics	E-Mail	Searc	h Book	mark								
Evidence Items		File Status	File Categ	ory	.0		n 😽 😽 🍃	a ina 🙆 (	ຄືເອົ					
vidence items:	2	KFF Alert Files: 0	Documents:	1449	-	_								_
File Items		Bookmarked items: 0	Spreadsheets:	27	and the second se		A STATEMENT			Contraction of the		AND IN THE OWNER		
otal File items: 500	00	Bad Extension: 112	Databases:	0	State of the second						C. Burger	and the second second		
hecked items:	0	Encrypted Files: 1	Graphics:	1664	and part of some						and the second	State State	131 9	2
Inchecked Items: 500	00	From E-mail: 0	Multimedia:	0	Contraction of the						Constant of the second		1000	
lagged Thumbnails:	0	Deleted Files: 2726	E-mail Messages	0	ALC: NO.						Sector Sector		100	
ther Thumbnails: 166	84	From Recycle Bin: 0	Executables:	0	100 - 10 - 10 - 10 - 10 - 10 - 10 - 10					Sal States		1 - 1 - 1 - 1	100	
ittered In: 500	00	Duplicate items: 790	Archives:	46	100			Carlos and	1000	A REAL PROPERTY AND INCOME.		1		
iltered Out:	0	OLE Subitems: 541	Folders:	26			-	and the second					10	
Unfiltered Filtered		Flagged Ignore: 0	Slack/Free Space			244	a state of the second					and the second second		
All items Actual File		KFF Ignorable: 0	Other Known Typ									0	21	
Par ing ing							A CONTRACTOR OF A DESCRIPTION OF A DESCRIPANTE A DESCRIPANTE A DESCRIPANTE A DESCRIPTION OF A DESCRIPTION OF					a success of the second second	>	č.
	3	Data Carved Files: 0	Unknown Type:	1411 All Co	Iumns Recycle Bi		otz File Type	Category	Subject	Cr Date	Mod Date	Acc Date	L-Size	
File Name		D V off Unfiltered	~		Recycle Bi	Ext	File Type	Category	Subject					12
File Name	3	V OFF Unfiltered     Full Path     Hdd image1\Part	L'estre service de la companya de la	All Co	Recycle Bi			Category Graphic Document	Subject	Cr Date 11/10/2018 4:44:16 PM N/A			L-Size 7,817,123 37,940	-
File Name	3	Unfiltered	_1\Bhargav Hdd-NT	All Co	Recycle Bi	Ext JPG	File Type JPEG/Exif file	Graphio	Subject	11/10/2018 4:44:16 PM	11/22/2015 2:02:18 AM N/A	11/10/2018 4:44:16 PM N/A	7,817,123	0
File Name MG_1754.JPG MG_1754.JPG.ht MG_1755.JPG	<u>3</u> €	Unfiltered Full Path Hdd image1/Part Hdd image1/Part Hdd image1/Part	_1\8hargav Hdd-N1 _1\8hargav Hdd-N1	FS\100CAN	Recycle Bi	Ext JPG htm	File Type JPEG/Exif file Hypertext Do	Graphic Document	Subject	11/10/2018 4:44:16 PM N/A	11/22/2015 2:02:18 AM N/A	11/10/2018 4:44:16 PM N/A	7,817,122	0
File Name MG_1754.JPG MG_1754.JPG.ht MG_1755.JPG MIG_1755.JPG.ht MG_1755.JPG.ht MG_1755.JPG	tm tm	Off Unfiltered      Full Path      Hdd image1/Part      Hdd image1/	_1\Bhargav Hdd-N1 _1\Bhargav Hdd-N1 _1\Bhargav Hdd-N1	FS/100CAN FS/100CAN FS/100CAN FS/100CAN	Recycle Bi	Ext JPG htm JPG	File Type JPEG/Exif file Hypertext Do JPEG/Exif file	Graphio Document Graphic	Subject	11/10/2018 4:44:16 PM N/A 11/10/2018 4:44:16 PM N/A	11/22/2015 2:02:18 AM N/A 11/22/2015 2:02:22 AM N/A	11/10/2018 4:44:16 PM N/A 11/10/2018 4:44:16 PM	7,817,123 37,940 7,788,925	0 5 3
<ul> <li>File Name</li> <li>MIG_1754.JPG</li> <li>MIG_1754.JPG.ht</li> <li>MIG_1755.JPG</li> <li>MIMG_1755.JPG.ht</li> <li>MIMG_1756.JPG</li> <li>MIMG_1756.JPG</li> <li>MIMG_1756.JPG.ht</li> </ul>	tm tm	Orf Unfiltered      Unfiltered      Full Path      Hdd image1Part      Hdd image1	118hargav Hdd-N1 118hargav Hdd-N1 118hargav Hdd-N1 118hargav Hdd-N1 118hargav Hdd-N1 118hargav Hdd-N1	All Co     FS/100CAN     FS/100CAN     FS/100CAN     FS/100CAN     FS/100CAN     FS/100CAN     FS/100CAN	Recycle Bi	Ext JPG htm JPG htm JPG htm	File Type JPEG/Exif file Hypertext Do JPEG/Exif file Hypertext Do JPEG/Exif file Hypertext Do	Graphic Document Graphic Document Graphic Document	Subject	11/10/2018 4:44:16 PM N/A 11/10/2018 4:44:16 PM N/A 11/10/2018 4:44:16 PM N/A	11/22/2015 2:02:18 AM N/A 11/22/2015 2:02:22 AM N/A 11/22/2015 2:29:38 AM N/A	11/10/2018 4:44:16 PM N/A 11/10/2018 4:44:16 PM N/A 11/10/2018 4:44:16 PM N/A	7,817,122 37,940 7,788,925 37,943 9,380,163 37,942	0 0 0 0 0
File Name File Name MIG_1754.JPG MIG_1754.JPG MIG_1755.JPG MIG_1755.JPG MIG_1755.JPG MIG_1755.JPG MIG_1756.JPG MIG_1756.JPG MIG_1756.JPG	tm tm	OF Unfiltered      OF Unfiltered      Full Path      Hdd image1Part      Hdd      Hdd image1Part      Hdd      Hdd image1Part      Hdd      Hdd	118hargav Hdd-N1 118hargav Hdd-N1 118hargav Hdd-N1 118hargav Hdd-N1 118hargav Hdd-N1 118hargav Hdd-N1 118hargav Hdd-N1	All Co     FS 100CAN	Recycle Bi	Ext JPG htm JPG htm JPG htm JPG	File Type JPEG/Exif file Hypertext Do JPEG/Exif file Hypertext Do JPEG/Exif file Hypertext Do JPEG/Exif file	Graphic Document Graphic Document Graphic Document Graphic	Subject	11/10/2018 4:44:16 PM N/A 11/10/2018 4:44:16 PM N/A 11/10/2018 4:44:16 PM N/A 11/10/2018 4:44:16 PM	11/22/2015 2:02:18 AM N/A 11/22/2015 2:02:22 AM N/A 11/22/2015 2:29:38 AM N/A 11/22/2015 2:30:12 AM	11/10/2018 4:44:16 PM N/A 11/10/2018 4:44:16 PM N/A 11/10/2018 4:44:16 PM N/A 11/10/2018 4:44:16 PM	7,817,122 37,940 7,788,925 37,943 9,380,103 37,943 6,524,333	0 15 13 13 12 12
File Name  File Name  MIG_1754.JPG MIG_1754.JPG MIG_1755.JPG MIG_1756.JPG MIG_1756.JPG MIG_1756.JPG MIG_1756.JPG MIG_1758.JPG MIG_1758.JPG.HI	tm tm	Or Unfittered     Unfittered     Hdd image1/Part     Hdd     Hdd image1/Part     Hdd     Hd     Hdd     Hd     Hdd     Hdd     Hd     Hdd	_1\Bhargav Hdd-N1 _1\Bhargav Hdd-N1 _1\Bhargav Hdd-N1 _1\Bhargav Hdd-N1 _1\Bhargav Hdd-N1 _1\Bhargav Hdd-N1 _1\Bhargav Hdd-N1 _1\Bhargav Hdd-N1	All Co     FS 100CAN	Recycle Bi	Ext JPG htm JPG htm JPG htm JPG htm	File Type JPEG/Exif file Hypertext Do JPEG/Exif file Hypertext Do JPEG/Exif file Hypertext Do	Graphic Document Graphic Document Graphic Document Graphic Document	Subject	11/10/2018 4:44:16 PM N/A 11/10/2018 4:44:16 PM N/A 11/10/2018 4:44:16 PM N/A 11/10/2018 4:44:16 PM N/A	11/22/2015 2:02:18 AM N/A 11/22/2015 2:02:22 AM N/A 11/22/2015 2:29:38 AM N/A 11/22/2015 2:30:12 AM N/A	11/10/2018 4:44:16 PM N/A 11/10/2018 4:44:16 PM N/A 11/10/2018 4:44:16 PM N/A 11/10/2018 4:44:16 PM N/A	7,817,121 37,940 7,788,925 37,943 9,380,163 37,942 8,524,333 37,938	0 5 3 3 2 2 8
file Name           IMG_1754.JPG.M           IMG_1754.JPG.M           IMG_1755.JPG.M           IMG_1755.JPG.M           IMG_1756.JPG.M           IMG_1756.JPG.M           IMG_1756.JPG.M           IMG_1756.JPG.M           IMG_1758.JPG.M           IMG_1758.JPG.M           IMG_1758.JPG.M           IMG_1758.JPG.M           IMG_1759.JPG.M	tm tm tm	Orr Unfittered     Full Path     Hold image 1/Part	118hargav Hdd-N1 118hargav Hdd-N1 118hargav Hdd-N1 118hargav Hdd-N1 118hargav Hdd-N1 118hargav Hdd-N1 118hargav Hdd-N1 118hargav Hdd-N1	All Co           FS/100CAN	Recycle Bi	Ext JPG htm JPG htm JPG htm JPG htm JPG	File Type JPEG/Exif file Hypertext Do JPEG/Exif file Hypertext Do JPEG/Exif file Hypertext Do JPEG/Exif file Hypertext Do JPEG/Exif file	Graphic Document Graphic Document Graphic Document Graphic Document Graphic	Subject	11/10/2018 4:44:16 PM N/A 11/10/2018 4:44:16 PM N/A 11/10/2018 4:44:16 PM N/A 11/10/2018 4:44:16 PM N/A 11/10/2018 4:44:17 PM	11/22/2015 2:02:18 AM N/A 11/22/2015 2:02:22 AM N/A 11/22/2015 2:29:38 AM N/A 11/22/2015 2:30:12 AM N/A 11/22/2015 2:31:16 AM	11/10/2018 4:44:16 PM N/A 11/10/2018 4:44:16 PM N/A 11/10/2018 4:44:16 PM N/A 11/10/2018 4:44:16 PM N/A 11/10/2018 4:44:17 PM	7,817,122 37,940 7,788,922 37,943 9,380,160 37,942 6,524,332 37,938 7,351,870	0 5 3 3 2 2 8 0
fie Name           MAG_1754.JPG           MIMG_1754.JPG           MIMG_1755.JPG	tm tm tm	Or Unftered     Unftered     Full Path     Hdd image1Part     Hdd	18hargav Hdd-N1 18hargav Hdd-N1 18hargav Hdd-N1 18hargav Hdd-N1 18hargav Hdd-N1 18hargav Hdd-N1 18hargav Hdd-N1 18hargav Hdd-N1 18hargav Hdd-N1	All Co           FS/100CAN	Recycle Bi	Ext JPG htm JPG htm JPG htm JPG htm	File Type JPEG/Exif file Hypertext Do JPEG/Exif file Hypertext Do JPEG/Exif file Hypertext Do JPEG/Exif file Hypertext Do	Graphic Document Graphic Document Graphic Document Graphic Document Graphic Document	Subject	11/10/2018 4:44:18 PM N/A 11/10/2018 4:44:18 PM N/A 11/10/2018 4:44:16 PM N/A 11/10/2018 4:44:16 PM N/A 11/10/2018 4:44:17 PM N/A	11/22/2015 2:02:18 AM N/A 11/22/2015 2:02:22 AM N/A 11/22/2015 2:29:38 AM N/A 11/22/2015 2:30:12 AM N/A 11/22/2015 2:31:16 AM N/A	11/10/2018 4:44:16 PM N/A 11/10/2018 4:44:16 PM N/A 11/10/2018 4:44:16 PM N/A 11/10/2018 4:44:16 PM N/A 11/10/2018 4:44:17 PM N/A	7,817,123 37,940 7,788,922 37,943 9,380,163 37,943 6,524,333 37,938 7,351,870 37,944	0 5 3 3 2 2 8 0 4
File Name           IM0_1754 JPG           IM0_1754 JPG           IM0_1755 JPG           IM0_1755 JPG           IM0_1758 JPG JPG           IM0_1758 JPG JPG           IM0_1750 JPG           IM0_1750 JPG           IM0_1750 JPG	tm tm tm tm	Or Unflered     Full Path     Hdd Image (Part     Hd Image (Part	18hargav Hdd-N1 18hargav Hdd-N1 18hargav Hdd-N1 18hargav Hdd-N1 18hargav Hdd-N1 18hargav Hdd-N1 18hargav Hdd-N1 18hargav Hdd-N1 18hargav Hdd-N1	All Co     F5/100CAN	Recycle Bi Recycle Bi Rec Rec Rec Rec Rec Rec Rec Rec	Ext JPG htm JPG htm JPG htm JPG htm JPG	File Type JPEG/Exit file Hypertext Do JPEG/Exit file Hypertext Do JPEG/Exit file Hypertext Do JPEG/Exit file Hypertext Do JPEG/Exit file	Graphio Document Graphic Document Graphic Document Graphic Document Graphic Document Graphic	Subject	11/10/2018 4:44:16 PM N/A 11/10/2018 4:44:16 PM N/A 11/10/2018 4:44:16 PM N/A 11/10/2018 4:44:16 PM N/A 11/10/2018 4:44:17 PM N/A 11/10/2018 4:44:17 PM	11/22/2015 2:02:18 AM N/A 11/22/2015 2:02:22 AM N/A 11/22/2015 2:29:38 AM N/A 11/22/2015 2:30:12 AM N/A 11/22/2015 2:31:16 AM N/A 11/22/2015 2:31:40 AM	11/10/2018 4:44:16 PM N/A 11/10/2018 4:44:16 PM N/A 11/10/2018 4:44:16 PM N/A 11/10/2018 4:44:16 PM N/A 11/10/2018 4:44:17 PM N/A 11/10/2018 4:44:17 PM	7,817,123 37,940 7,788,924 9,380,160 37,943 6,524,333 37,933 7,351,870 37,944 6,921,874	0 5 3 3 2 2 8 0 4 4
File Name           MA0_1764 JPG           MM0_1765 JPG           MM0_1769 JPG           MM0_1769 JPG           MM0_1769 JPG           MM0_1769 JPG	tm tm tm tm	Or Unflered     Full Path     Hdd Image1Part     Hd     Hd     HdImage1Part     Hd     Hd     Hd     Hd	18hargav Hdd-N1 18hargav Hdd-N1	FS:100CAN	Recycle Bi	Ext JPG htm JPG htm JPG htm JPG htm JPG htm	File Type JPEG/Exif file Hypertext Do. JPEG/Exif file Hypertext Do. JPEG/Exif file Hypertext Do. JPEG/Exif file Hypertext Do. JPEG/Exif file Hypertext Do.	Graphio Document Graphic Document Graphic Document Graphic Document Graphic Document Graphic	Subject	11/10/2018 4-44-16 PM NA 11/10/2018 4-44-16 PM NA 11/10/2018 4-44-16 PM NA 11/10/2018 4-44-17 PM NA 11/10/2018 4-44-17 PM NA	11/22/2015 2:02:18 AM NA 11/22/2015 2:02:22 AM NA 11/22/2015 2:29:38 AM NA 11/22/2015 2:30:12 AM NA 11/22/2015 2:31:16 AM NA NA	11/10/2018 4:44:16 PM N/A 11/10/2018 4:44:16 PM N/A 11/10/2018 4:44:16 PM N/A 11/10/2018 4:44:16 PM N/A 11/10/2018 4:44:17 PM N/A N/A	7,817,122 37,940 7,788,925 37,940 9,380,100 37,940 8,524,330 37,954 7,351,870 37,944 6,921,874 37,941	0 5 3 3 2 2 8 0 4 4 1
File Name           Image: Mage: 1764. JPG           Image: 1765. JPG           Image: 176	tm tm tm tm tm	Very orr Unfiltered     Full Path     Hdd image (Part     Hd image (Part	18hargav Hdd-N1 18hargav Hdd-N1 18hargav Hdd-N1 18hargav Hdd-N1 18hargav Hdd-N1 18hargav Hdd-N1 18hargav Hdd-N1 18hargav Hdd-N1 18hargav Hdd-N1	All Co     F5/100CAN	Recycle Bi	Ext JPG htm JPG htm JPG htm JPG htm JPG	File Type JPEG/Exit file Hypertext Do JPEG/Exit file Hypertext Do JPEG/Exit file Hypertext Do JPEG/Exit file Hypertext Do JPEG/Exit file	Graphio Document Graphic Document Graphic Document Graphic Document Graphic Document Graphic	Subject	11/10/2018 4:44:16 PM N/A 11/10/2018 4:44:16 PM N/A 11/10/2018 4:44:16 PM N/A 11/10/2018 4:44:16 PM N/A 11/10/2018 4:44:17 PM N/A 11/10/2018 4:44:17 PM	11/22/2015 2:02:18 AM NA 11/22/2015 2:02:22 AM NA 11/22/2015 2:29:38 AM NA 11/22/2015 2:30:12 AM NA 11/22/2015 2:31:16 AM NA NA	11/10/2018 4:44:16 PM N/A 11/10/2018 4:44:16 PM N/A 11/10/2018 4:44:16 PM N/A 11/10/2018 4:44:16 PM N/A 11/10/2018 4:44:17 PM N/A N/A	7,817,123 37,940 7,788,924 9,380,160 37,943 6,524,333 37,933 7,351,870 37,944 6,921,874	0 5 3 3 2 2 8 0 4 4 1 1
File Name           If M0_1754.JP0           M0_1754.JP0           M0_1756.JP0           M0_1756.JP0           M0_1756.JP0           M0_1756.JP0           M0_1756.JP0           M0_1756.JP0           M0_1756.JP0           M0_1756.JP0           M0_1758.JP0           M0_1759.JP0           M0_1759.JP0           M0_1759.JP0           M0_1759.JP0           M0_1751.JP0.JP0           M0_1751.JP0.JP1	tm tm tm tm tm	Or Unfleted     Or Unfleted     Full Path     Hdd Image1Part	18hargav Hdd-N1 18hargav Hdd-N1	All Co           F5/100CAN	Recycle Bi	Ext JPG htm JPG htm JPG htm JPG htm JPG htm JPG	File Type JPEG/Exif file Hypertext Do JPEG/Exif file Hypertext Do JPEG/Exif file Hypertext Do JPEG/Exif file Hypertext Do JPEG/Exif file JPEG/Exif file	Graphic Document Graphic Document Graphic Document Graphic Document Graphic Document Graphic Document Graphic	Subject	11102018 4.44.16 PM NA 11102018 4.44.16 PM NA 11102018 4.44.16 PM NA 11102018 4.44.16 PM NA 11102018 4.44.17 PM NA 11102018 4.44.17 PM NA	11/22/2015 2:02:18 AM NA 11/22/2015 2:02:22 AM NA 11/22/2015 2:29:38 AM NA 11/22/2015 2:30:12 AM NA NA 11/22/2015 2:31:16 AM NA 11/22/2015 2:31:50 AM NA	11/10/2018 4.44.16 PM N/A 11/10/2018 4.44.16 PM N/A 11/10/2018 4.44.16 PM N/A 11/10/2018 4.44.16 PM N/A 11/10/2018 4.44.17 PM N/A 11/10/2018 4.44.17 PM	7,817,122 37,944 7,788,925 37,945 9,380,163 37,944 6,524,333 7,351,870 37,944 6,921,874 37,944 7,067,474	0 5 3 3 2 2 8 0 4 4 1 1 8
file Name           IMG_1754.JPG.M           IMG_1754.JPG.M           IMG_1755.JPG.M           IMG_1755.JPG.M           IMG_1756.JPG.M           IMG_1756.JPG.M           IMG_1756.JPG.M           IMG_1756.JPG.M           IMG_1758.JPG.M           IMG_1758.JPG.M           IMG_1758.JPG.M           IMG_1758.JPG.M           IMG_1759.JPG.M	tm tm tm tm tm tm	Very orr Unfiltered     Full Path     Hod image (Part     Hod	18hargav Hdd-NT 18hargav Hdd-NT	All Co           F5:100CAN           F5:100CAN	Recycle Bi           ka           ka      <	Ext JPG htm JPG htm JPG htm JPG htm JPG htm JPG htm	File Type JPEG/Esti file Hypertext Do JPEG/Esti file Hypertext Do JPEG/Esti file Hypertext Do JPEG/Esti file Hypertext Do JPEG/Esti file Hypertext Do JPEG/Esti file Hypertext Do	Graphic Document Graphic Document Graphic Document Graphic Document Graphic Document Graphic Document Graphic Document	Subject	11102018 4.44.16 PM NA 11102018 4.44.16 PM NA 11102018 4.44.16 PM NA 11102018 4.44.16 PM NA 11102018 4.44.17 PM NA 11102018 4.44.17 PM NA	11/22/2015 2:02:18 AM NA 11/22/2015 2:02:22 AM NA 11/22/2015 2:29:38 AM NA 11/22/2015 2:30:12 AM NA NA 11/22/2015 2:31:16 AM NA 11/22/2015 2:31:50 AM NA	11/10/2018 4:44:16 PM N/A 11/10/2018 4:44:16 PM N/A 11/10/2018 4:44:16 PM N/A 11/10/2018 4:44:16 PM N/A 11/10/2018 4:44:17 PM N/A 11/10/2018 4:44:17 PM N/A	7,817,122 37,940 7,788,924 37,943 9,380,160 37,943 6,524,333 37,943 7,351,870 37,944 6,921,874 37,944 7,067,471 37,938	0 5 3 3 2 2 8 0 4 4 1 1 8 9

Figure 83. Image Preview for HDD Image

Overview E	xplore	Graphics	E-Mail	Search Bo	okmark								
Evidence Items		File Status	File Categor	ny A		1 20 20 20	i i i i i i i i i i i i i i i i i i i	1					
vidence items:	2 KFF	Alert Files: 0	Documents:	1449	-					A REAL PROPERTY OF			1
File Items	Boo	kmarked Items: 0	Spreadsheets:	27			2 23	6 A.		1 10 10		10.00	2
otal File items: 500	00 Bad	Extension: 112	Databases:	0		100		Sec. 1				10 miles	1
Checked Items:	0 Enci	ypted Files: 1	Graphics:	1664	1 a		1 tor	- Aller	1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	1 1 1	A ME S		
Inchecked Items: 500	00 From	n E-mail: 0	Multimedia:	0	7 E	R. 6 . 7	2.30	6	and a start of the second	111		<b>2</b> 565	3
lagged Thumbnails:	0 Dele	ted Files: 2726	E-mail Messages:	0			112	A little at		Caller -	- 533	1000	
Other Thumbnails: 166	64 From	Recycle Bin: 0	Executables:	0	1.00	12-12-1			A DUAL AL	1119			
itered In: 50		icate Items; 790	Archives:	46	20	-	1	and a lot	and the second second		1000 11		
itered Out		Subitems: 541	Folders:	26	En.	1		1	and the second	The second second		500	
Unfiltered Filtered		ged Ignore: 0	Slack/Free Space:	182		-	1	A 2	1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	1000		A. C. C.	
All Items Actual File		ignorable: 0	Other Known Type		( and	1992	and the second			San Karal		0.0	
All items Actual File	spinster . Transaction and	Carved Files: 0	Unknown Type:	1411		100 C 100 C		1.00		10			
	B <u></u>	GFF Unfiltered	~ 1	All Columns Recycle Bi	~	DTZ File Type	Category	Subject	Cr Date	Mod Date	Acc Date	L-Size	_
File Name		Full Path		Recycle Bi	Ext	File Type		Subject					
File Name	bender-30	Full Path 41 Hdd image1\Par	t_1\Bhargav Hdd-NTF	Recycle Bi	Ext	File Type JPEG/JFIF File	Graphic	Subject	11/10/2018 4:37:52 PM	9/30/2018 1:00:52 PM	11/10/2018 4:37:52 PM	1,365,88	
File Name	bender-30 is-97263-u	Full Path 41 Hdd image1\Par nsp Hdd image1\Par	t_1\Bhargav Hdd-NTF t_1\Bhargav Hdd-NTF	Recycle Bi SISRECYC SISRECYC	Ext ipg ipg	File Type JPEG/JFIF File JPEG/JFIF File	Graphic Graphic	Subject	11/10/2018 4:37:52 PM 11/10/2018 4:37:05 PM	9/30/2018 1:00:52 PM 9/30/2018 2:21:02 PM	11/10/2018 4:37:52 PM 11/10/2018 4:37:05 PM	1,365,88	17
File Name	bender-30 is-97263-u 3105-unsp	Full Path 41 Hdd image1\Par ash Hdd image1\Par ash Hdd image1\Par	t_1\Bhargav Hdd-NTF t_1\Bhargav Hdd-NTF t_1\Bhargav Hdd-NTF	Recycle Bi SISRECYC SISRECYC SISRECYC	Ext ipg ipg ipg	File Type JPEG/JFIF File JPEG/JFIF File JPEG/JFIF File	Graphic Graphic Graphic	Subject	11/10/2018 4:37:52 PM 11/10/2018 4:37:05 PM 11/10/2018 4:37:05 PM	9/30/2018 1:00:52 PM 9/30/2018 2:21:02 PM 9/30/2018 2:16:50 PM	11/10/2018 4:37:52 PM 11/10/2018 4:37:05 PM 11/10/2018 4:37:05 PM	1,365,88 963,41 3,068,51	17
File Name	bender-30 is-97263-u 3105-unsp i637-unspl	Full Path 41 Hdd image1\Pan nsp Hdd image1\Pan ash Hdd image1\Pan ash Hdd image1\Pan	t_1\Bhargav Hdd-NTF t_1\Bhargav Hdd-NTF t_1\Bhargav Hdd-NTF t_1\Bhargav Hdd-NTF	Recycle Bi SISRECYC SISRECYC SISRECYC SISRECYC	iP9 iP9 iP9 iP9 iP9	File Type JPEG/JFIF File JPEG/JFIF File JPEG/JFIF File JPEG/JFIF File	Graphic Graphic Graphic Graphic	Subject	11/10/2018 4:37:52 PM 11/10/2018 4:37:05 PM 11/10/2018 4:37:05 PM 11/10/2018 4:37:05 PM 11/10/2018 4:37:52 PM	9/30/2018 1:00:52 PM 9/30/2018 2:21:02 PM 9/30/2018 2:16:50 PM 9/30/2018 1:06:34 PM	11/10/2018 4:37:52 PM 11/10/2018 4:37:05 PM	1,365,88	17 10 39
File Name	bender-30 is-97263-u 9106-unsp i637-unspl	Full Path Hdd image1\Par nsp Hdd image1\Par ash Hdd image1\Par ash Hdd image1\Par ash Hdd image1\Par sh Hdd image1\Par	t_1\Bhargav Hdd-NTF t_1\Bhargav Hdd-NTF t_1\Bhargav Hdd-NTF t_1\Bhargav Hdd-NTF t_1\Bhargav Hdd-NTF t_1\Bhargav Hdd-NTF	Recycle Bi SISRECYC SISRECYC SISRECYC SISRECYC SISRECYC	IPG IPG IPG IPG IPG IPG	File Type JPEG/JFIF File JPEG/JFIF File JPEG/JFIF File JPEG/JFIF File	Graphic Graphic Graphic Graphic Graphic	Subject	11/10/2018 4:37:52 PM 11/10/2018 4:37:05 PM 11/10/2018 4:37:05 PM 11/10/2018 4:37:05 PM 11/10/2018 4:37:52 PM 11/10/2018 4:37:52 PM	9/30/2018 1:00:52 PM 9/30/2018 2:21:02 PM 9/30/2018 2:16:50 PM 9/30/2018 1:06:34 PM 9/30/2018 1:06:52 PM	11/10/2018 4:37:52 PM 11/10/2018 4:37:05 PM 11/10/2018 4:37:05 PM 11/10/2018 4:37:05 PM 11/10/2018 4:37:52 PM 11/10/2018 4:37:52 PM	1,365,88 963,41 3,068,51 4,075,83 4,075,83	17 10 39
File Name	bender-30 is-97263-u 105-unsp i637-unsp i637-unsp 1864-unsp	Full Path Hdd image1\Pari ash Hdd image1\Pari ash Hdd image1\Pari ash Hdd image1\Pari ash Hdd image1\Pari las Hdd image1\Pari	t_1\Bhargav Hdd-NTF t_1\Bhargav Hdd-NTF t_1\Bhargav Hdd-NTF t_1\Bhargav Hdd-NTF	Recycle Bi SISRECYC SISRECYC SISRECYC SISRECYC SISRECYC	iP9 iP9 iP9 iP9 iP9	File Type JPEG/JFIF File JPEG/JFIF File JPEG/JFIF File JPEG/JFIF File	Graphic Graphic Graphic Graphic Graphic Graphic	Subject	11/10/2018 4:37:52 PM 11/10/2018 4:37:05 PM 11/10/2018 4:37:05 PM 11/10/2018 4:37:05 PM 11/10/2018 4:37:52 PM	9/30/2018 1:00:52 PM 9/30/2018 2:21:02 PM 9/30/2018 2:16:50 PM 9/30/2018 1:06:34 PM 9/30/2018 1:05:52 PM 9/30/2018 1:56:58 PM	11/10/2018 4:37:52 PM 11/10/2018 4:37:05 PM 11/10/2018 4:37:05 PM 11/10/2018 4:37:05 PM 11/10/2018 4:37:52 PM	1,365,88 963,41 3,068,51 4,075,83	17 10 39 39 00
File Name ngaere-woodford- inicholas-kampouri nick-karvounis-160 nick-scheerbart-16 nick-scheerbart-16 nick-scheerbart-16 nick-scheerbart-16 oldskool-photogra	bender-30 is-97263-u 105-unsp 1637-unspl 1864-unsp phy-1765	Full Path 41 Hdd image1\Pari ash Hdd image1\Pari ash Hdd image1\Pari ash Hdd image1\Pari ash Hdd image1\Pari 76 Hdd image1\Pari 76	t_1\Bhargav Hdd-NTF t_1\Bhargav Hdd-NTF t_1\Bhargav Hdd-NTF t_1\Bhargav Hdd-NTF t_1\Bhargav Hdd-NTF t_1\Bhargav Hdd-NTF	Recycle Bi SISRECYC SISRECYC SISRECYC SISRECYC SISRECYC SISRECYC	Ext ipg ipg ipg ipg ipg ipg	File Type JPEG/JFIF File JPEG/JFIF File JPEG/JFIF File JPEG/JFIF File JPEG/JFIF File	Graphic Graphic Graphic Graphic Graphic Graphic	Subject	11/10/2018 4:37:52 PM 11/10/2018 4:37:55 PM 11/10/2018 4:37:05 PM 11/10/2018 4:37:52 PM 11/10/2018 4:37:52 PM 11/10/2018 4:37:52 PM	9/30/2018 1:00:52 PM 9/30/2018 2:21:02 PM 9/30/2018 2:16:50 PM 9/30/2018 1:06:34 PM 9/30/2018 1:05:52 PM 9/30/2018 1:56:58 PM 9/30/2018 1:04:54 PM	11/10/2018 4:37:52 PM 11/10/2018 4:37:05 PM 11/10/2018 4:37:05 PM 11/10/2018 4:37:52 PM 11/10/2018 4:37:52 PM 11/10/2018 4:37:53 PM	1,365,88 963,41 3,068,51 4,075,83 4,075,83 3,893,00	17 10 39 39 00 01
File Name	bender-30 is-97263-u 9106-unsp 637-unsp 637-unsp 837-unsp 1864-unsp phy-1765 -666498-u	Full Path Full Path 41 Hdd image1/Pari ash Hdd image1/Pari ash Hdd image1/Pari las Hdd image1/Pari 78 Hdd image1/Pari 78 Hdd image1/Pari	t_1\Bhargav Hdd-NTF t_1\Bhargav Hdd-NTF t_1\Bhargav Hdd-NTF t_1\Bhargav Hdd-NTF t_1\Bhargav Hdd-NTF t_1\Bhargav Hdd-NTF t_1\Bhargav Hdd-NTF	Recycle Bi SISRECYC SISRECYC SISRECYC SISRECYC SISRECYC SISRECYC SISRECYC	Ext ipg ipg ipg ipg ipg ipg ipg	File Type JPEG/JFIF File JPEG/JFIF File JPEG/JFIF File JPEG/JFIF File JPEG/JFIF File JPEG/JFIF File	Graphic Graphic Graphic Graphic Graphic Graphic Graphic	Subject	11/10/2018 4:37:52 PM 11/10/2018 4:37:05 PM 11/10/2018 4:37:05 PM 11/10/2018 4:37:52 PM 11/10/2018 4:37:52 PM 11/10/2018 4:37:53 PM 11/10/2018 4:37:53 PM	9/30/2018 1:00:52 PM 9/30/2018 2:21:02 PM 9/30/2018 2:10:50 PM 9/30/2018 1:06:54 PM 9/30/2018 1:06:55 PM 9/30/2018 1:06:55 PM 9/30/2018 1:06:56 PM 9/30/2018 1:09:54 PM	11/10/2018 4:37:52 PM 11/10/2018 4:37:05 PM 11/10/2018 4:37:05 PM 11/10/2018 4:37:52 PM 11/10/2018 4:37:52 PM 11/10/2018 4:37:53 PM 11/10/2018 4:37:53 PM	1,365,88 963,41 3,068,51 4,075,83 4,075,83 3,893,00 2,730,50	17 10 39 39 00 01 67
File Name File Name nick-tanounis 165 nick-scheerbart 15 nick-scheerbart 15 nick-	bender-30 is-97263-u 106-unsp 637-unsp 637-unsp 1864-unsp phy-1765 -005498-u 243278-ur	Full Path Hdd image1Par nsp Hdd image1Par ash Hdd image1Par ash Hdd image1Par las Hdd image1Par risp Hdd image1Par nsp Hdd image1Par	t_118hargav Hdd-NTFF 118hargav Hdd-NTFF 118hargav Hdd-NTFF 118hargav Hdd-NTFF 118hargav Hdd-NTFF 118hargav Hdd-NTFF 118hargav Hdd-NTFF 118hargav Hdd-NTFF	Recycle Bi SISRECYC SISRECYC SISRECYC SISRECYC SISRECYC SISRECYC SISRECYC SISRECYC	Ext ipg ipg ipg ipg ipg ipg ipg ipg	File Type JPEG/JFIF File JPEG/JFIF File JPEG/JFIF File JPEG/JFIF File JPEG/JFIF File JPEG/JFIF File JPEG/JFIF File	Graphic Graphic Graphic Graphic Graphic Graphic Graphic Graphic	Subject	11/10/2018 4:37:52 PM 11/10/2018 4:37:05 PM 11/10/2018 4:37:52 PM 11/10/2018 4:37:52 PM 11/10/2018 4:37:52 PM 11/10/2018 4:37:53 PM 11/10/2018 4:37:53 PM	9/30/2018 1:00:52 PM 9/30/2018 2:21:02 PM 9/30/2018 2:16:50 PM 9/30/2018 1:06:34 PM 9/30/2018 1:06:52 PM 9/30/2018 1:06:54 PM 9/30/2018 1:04:54 PM 9/30/2018 1:39:54 PM 9/30/2018 1:39:55 PM	11/10/2018 4:37:52 PM 11/10/2018 4:37:05 PM 11/10/2018 4:37:05 PM 11/10/2018 4:37:52 PM 11/10/2018 4:37:52 PM 11/10/2018 4:37:53 PM 11/10/2018 4:37:53 PM	1,365,88 963,41 3,068,61 4,075,83 4,075,83 3,893,00 2,730,60 204,06	17 10 39 39 00 01 67 26
File Name     ngaers-woodford-     nicholas-kampour     nich-tanvonis-156     nick-scheerbart-15     nick-scheerbart-15     nick-scheerbart-16     nick-scheerbart-16     olds-jorgar-241     oldskool-photogra     ole-jorgar-bakkan     pablo-heimplatz-2     patic-brinkama-3	bender-30 is-97263-u 3105-unspl 637-unspl 1864-unsp phy-1765 -666498-u 243278-ur 60603-uns	Full Path Hdd image1Pan ash Hdd image1Pan ash Hdd image1Pan ash Hdd image1Pan ash Hdd image1Pan 78 Hdd image1Pan nsp Hdd image1Pan spl Hdd image1Pan	t_1\Bhargav Hdd-NTF: t_1\Bhargav Hdd-NTF: t_1\Bhargav Hdd-NTF: t_1\Bhargav Hdd-NTF: t_1\Bhargav Hdd-NTF: t_1\Bhargav Hdd-NTF: t_1\Bhargav Hdd-NTF: t_1\Bhargav Hdd-NTF:	Recycle Bi           SIGRECYC         SIGRECYC           SIGRECYC         SIGRECYC           SIGRECYC         SIGRECYC           SIGRECYC         SIGRECYC           SIGRECYC         SIGRECYC           SIGRECYC	Ext jpg jpg jpg jpg jpg jpg jpg jpg jpg	File Type JPEG/JFIF File JPEG/JFIF File JPEG/JFIF File JPEG/JFIF File JPEG/JFIF File JPEG/JFIF File JPEG/JFIF File	Graphic Graphic Graphic Graphic Graphic Graphic Graphic Graphic Graphic Graphic	Subject	11/10/2018 4:37:52 PM 11/10/2018 4:37:05 PM 11/10/2018 4:37:05 PM 11/10/2018 4:37:52 PM 11/10/2018 4:37:52 PM 11/10/2018 4:37:53 PM 11/10/2018 4:37:53 PM 11/10/2018 4:37:53 PM	9/30/2018 1 00:52 PM 9/30/2018 2 21:02 PM 9/30/2018 2 21:02 PM 9/30/2018 2 1:61:50 PM 9/30/2018 1 0:65 2 PM 9/30/2018 1 0:65 2 PM 9/30/2018 1 0:455 PM 9/30/2018 1 0:455 PM 9/30/2018 1 0:355 PM 9/30/2018 1 0:355 PM	11/10/2018 4:37:52 PM 11/10/2018 4:37:05 PM 11/10/2018 4:37:05 PM 11/10/2018 4:37:52 PM 11/10/2018 4:37:52 PM 11/10/2018 4:37:53 PM 11/10/2018 4:37:53 PM 11/10/2018 4:37:53 PM	1,365,88 963,41 3,068,61 4,075,83 4,075,83 3,893,00 2,730,50 204,00 1,604,22	17 10 39 39 00 01 67 26 44
File Name     ngaere-woodford-     nicholas-kampour     nick-akampour     nick-akampour     nick-aknerbart-15     rick-scheerbart-15	bender-30 is-97263-u 1105-unsp i637-unsp i637-unsp i837-unsp i854-unsp phy-1765 -665498-u 243278-ur 60503-uns 60377-unsp i	Full Path Hdd image1Pari nsp Hdd image1Pari ash Hdd image1Pari ash Hdd image1Pari ash Hdd image1Pari nsp Hdd image1Pari nsp Hdd image1Pari nsp	t_1\Bhargav Hdd-NTF t_1\Bhargav Hdd-NTF t_1\Bhargav Hdd-NTF t_1\Bhargav Hdd-NTF t_1\Bhargav Hdd-NTF t_1\Bhargav Hdd-NTF t_1\Bhargav Hdd-NTF t_1\Bhargav Hdd-NTF t_1\Bhargav Hdd-NTF	Recycle Bi SIGRECYC SIGRECYC SIGRECYC SIGRECYC SIGRECYC SIGRECYC SIGRECYC SIGRECYC	III Ext ipg ipg ipg ipg ipg ipg ipg ipg	File Type JPEQ/JFIF File JPEG/JFIF File JPEG/JFIF File JPEG/JFIF File JPEG/JFIF File JPEG/JFIF File JPEG/JFIF File JPEG/JFIF File	Graphic Graphic Graphic Graphic Graphic Graphic Graphic Graphic Graphic Graphic Graphic	Subject	11/10/2018 4:37:52 PM 11/10/2018 4:37:55 PM 11/10/2018 4:37:55 PM 11/10/2018 4:37:52 PM 11/10/2018 4:37:52 PM 11/10/2018 4:37:53 PM 11/10/2018 4:37:53 PM 11/10/2018 4:37:55 PM 11/10/2018 4:37:55 PM	8/30/2018 1 00:52 PM 9/30/2018 2 21:02 PM 9/30/2018 2 1:0:50 PM 9/30/2018 1 0:0:54 PM 9/30/2018 1 0:0:52 PM 9/30/2018 1 0:55 PM 9/30/2018 1 0:55 PM 9/30/2018 1 0:358 PM 9/30/2018 1 1:0:55 PM	11/10/2018 4:37:52 PM 11/10/2018 4:37:05 PM 11/10/2018 4:37:05 PM 11/10/2018 4:37:52 PM 11/10/2018 4:37:52 PM 11/10/2018 4:37:53 PM 11/10/2018 4:37:53 PM 11/10/2018 4:37:53 PM 11/10/2018 4:37:55 PM	1,365,85 983,41 3,008,61 4,075,83 4,075,83 3,893,00 2,730,50 204,00 1,604,22 2,671,64	17 10 39 39 00 01 67 26 44 99
Fie Name	bender-30 is-97263-u 105-unsp 1637-unsp 1864-unsp phy-1765 666488-u 243278-ur 60503-un: 60377-unsp 2622-unsp 72147-unsp	Full Path           41         Hdd imaget iPari           nsp         Hdd imaget iPari           ash         Hdd imaget iPari           ash         Hdd imaget iPari           ash         Hdd imaget iPari           namoet iPari         Hdd imaget iPari           had imaget iPari         Hdd imaget iPari           namoet iPari         Hdd imaget iPari           namoet iPari         Hdd imaget iPari           hdd imaget iPari         Hdd imaget iPari           hdd imaget iPari         Hdd imaget iPari           namoet iPari         Hdd imaget iPari	L_1Bhagav HddATFF L_1Bhagav HddATFF	Recycle Bi           SIRECYC	Ext ipg ipg ipg ipg ipg ipg ipg ipg	File Type JPEG/JFIF File JPEG/JFIF File JPEG/JFIF File JPEG/JFIF File JPEG/JFIF File JPEG/JFIF File JPEG/JFIF File JPEG/JFIF File JPEG/JFIF File JPEG/JFIF File	Graphic Graphic Graphic Graphic Graphic Graphic Graphic Graphic Graphic Graphic Graphic	Subject	11/10/2018 4:37:62 PM 11/10/2018 4:37:62 PM 11/10/2018 4:37:62 PM 11/10/2018 4:37:62 PM 11/10/2018 4:37:62 PM 11/10/2018 4:37:63 PM 11/10/2018 4:37:53 PM 11/10/2018 4:37:53 PM 11/10/2018 4:37:55 PM 11/10/2018 4:37:55 PM	9/30/2018 1:00:52 PM 9/30/2018 2:21:02 PM 9/30/2018 2:16:50 PM 9/30/2018 1:06:54 PM 9/30/2018 1:06:56 PM 9/30/2018 1:06:56 PM 9/30/2018 1:04:54 PM 9/30/2018 1:04:56 PM	11/10/2018 4.37 62 PM 11/10/2018 4.37 65 PM 11/10/2018 4.37 65 PM 11/10/2018 4.37 65 PM 11/10/2018 4.37 62 PM 11/10/2018 4.37 63 PM 11/10/2018 4.37 63 PM 11/10/2018 4.37 63 PM 11/10/2018 4.37 65 PM 11/10/2018 4.37 65 PM 11/10/2018 4.37 65 PM	1,365,88 983,41 3,068,61 4,075,83 4,075,83 3,893,00 2,730,50 204,00 1,604,22 2,671,64 865,55 2,437,68 7,565,78	17 10 39 39 00 01 67 26 44 99 87 86
f File Name ngaene-woodford- in indu-tals-ampoun- inide.amounts-166 inide.amounts	bender-30 is-97263-u 8105-unsp 6837-unsp 1864-unsp phy-1765 -665498-u 665498-u 666593-unsp 60503-unsp 72122-unsp 72147-unsp 19330-uns	Full Path           41	t_1\Bhargav Hdd-NTF; _1\Bhargav Hdd-NTF;	Recycle Bi           SIRECYC	Ext ipg ipg ipg ipg ipg ipg ipg ipg	File Type JPEG/JFIF File JPEG/JFIF File JPEG/JFIF File JPEG/JFIF File JPEG/JFIF File JPEG/JFIF File JPEG/JFIF File JPEG/JFIF File JPEG/JFIF File JPEG/JFIF File	Graphic Graphic Graphic Graphic Graphic Graphic Graphic Graphic Graphic Graphic Graphic Graphic	Subject	11/10/2018 4:37:62 PM 11/10/2018 4:37:62 PM 11/10/2018 4:37:62 PM 11/10/2018 4:37:62 PM 11/10/2018 4:37:63 PM 11/10/2018 4:37:63 PM 11/10/2018 4:37:53 PM 11/10/2018 4:37:55 PM 11/10/2018 4:37:55 PM	9/30/2018 1:00:52 PM 9/30/2018 2:21:02 PM 9/30/2018 2:16:50 PM 9/30/2018 1:06:54 PM 9/30/2018 1:06:56 PM 9/30/2018 1:06:56 PM 9/30/2018 1:04:54 PM 9/30/2018 1:04:56 PM	11/10/2018 4:37 65 PM 11/10/2018 4:37 65 PM 11/10/2018 4:37 65 PM 11/10/2018 4:37 65 PM 11/10/2018 4:37 55 PM 11/10/2018 4:37 55 PM 11/10/2018 4:37 55 PM 11/10/2018 4:37 55 PM 11/10/2018 4:37 65 PM 11/10/2018 4:37 65 PM	1,365,88 963,41 3,068,51 4,075,83 4,075,83 3,893,00 2,730,56 204,00 1,604,22 2,671,64 865,55 2,437,65 7,555,76 2,372,24	17 10 39 39 00 01 67 26 44 99 87 86 40
1 File Name in choise kampour inicholas kampour inichalas kampour inickateurunis töö inickateurunis töö inickateuruni	bender-30 is-97263-u 1105-unsp 1105-unsp 11864-unsp phy-1765 -005488-u 243278-ur 605488-u 243278-ur 60503-un 60377-un 24322-unsp 72147-uns 19330-uns 383310-u	Full Path           41	L IBhagaw HdoATTF L IBhagaw HdoATTF	Recycle Bit           SIGNECYC	Ext jpg jpg jpg jpg jpg jpg jpg jpg jpg jpg	File Type JPEG/JFIF File JPEG/JFIF File	Graphic Graphic Graphic Graphic Graphic Graphic Graphic Graphic Graphic Graphic Graphic Graphic Graphic Graphic Graphic Graphic	Subject	11/10/2018 4:37:62 PM 11/10/2018 4:37:62 PM 11/10/2018 4:37:62 PM 11/10/2018 4:37:62 PM 11/10/2018 4:37:62 PM 11/10/2018 4:37:63 PM 11/10/2018 4:37:53 PM 11/10/2018 4:37:53 PM 11/10/2018 4:37:55 PM 11/10/2018 4:37:55 PM	9/30/2018 1 00:52 PM 9/30/2018 2 21:02 PM 9/30/2018 2 16:50 PM 9/30/2018 1 06:34 PM 9/30/2018 1 06:34 PM 9/30/2018 1 06:35 PM 9/30/2018 1 06:35 PM 9/30/2018 1 09:36 PM 9/30/2018 2 19:36 PM 9/30/2018 2 19:36 PM 9/30/2018 2 4:54 PM	11/10/2018 4.37 62 PM 11/10/2018 4.37 65 PM 11/10/2018 4.37 65 PM 11/10/2018 4.37 65 PM 11/10/2018 4.37 62 PM 11/10/2018 4.37 63 PM 11/10/2018 4.37 63 PM 11/10/2018 4.37 63 PM 11/10/2018 4.37 65 PM 11/10/2018 4.37 65 PM 11/10/2018 4.37 65 PM	1,365,88 963,41 3,068,51 4,075,83 4,075,83 3,893,00 2,730,65 2,24,00 1,604,22 2,671,64 865,55 2,437,68 7,565,75 2,372,24 1,633,11	17 10 39 00 01 67 26 44 99 87 86 40 10
Fie Name ngaer-woodford- nichtlas-kampoun inick-las-kampoun inick-karobestri nick-cherbert-16 ni	bender-30 is-97263-u 1105-unsp 1637-unsp 1884-unsp phy-1765 -665498-u 265498-u 265498-u 265498-u 2659-unsp 19320-uns 19330-uns 19330-uns 19330-uns	Full Path           41	L_1Bhargav HddATFF (_1Bhargav HddATFF	Recycle Bit           Starteryc           Starteryc	Ext jpg jpg jpg jpg jpg jpg jpg jpg jpg jpg	File Type JPEG/JFIF File JPEG/JFIF File	Graphic Graphic	Subject	11/10/2018 4.37.62 PM 11/10/2018 4.37.65 PM	9/30/2018 1:00:52 PM 9/30/2018 2:21:02 PM 9/30/2018 2:01:50 PM 9/30/2018 1:06:34 PM 9/30/2018 1:06:34 PM 9/30/2018 1:06:52 PM	11/10/2018 4:37 65 PM 11/10/2018 4:38 05 PM 11/10/2018 4:38 05 PM	1,365,88 963,41 3,068,51 4,075,83 4,075,83 3,893,00 2,730,56 204,00 1,604,22 2,671,64 865,55 2,437,65 7,555,76 2,372,24	17 10 39 39 00 01 67 26 44 99 87 86 40 10 43

Figure 84. Image Preview 2 for HDD Image

Overview	Explo	re Graphics	E-Mail	Searc	h Book	mark								
Evidence Ite	ems	File Status	File Catego	ry	0	- A	<b>P9 🚔 </b>		5) <b>(</b> 1)					
Evidence Items:	2	KFF Alert Files: 0	Documents:	1449		1.00								-
File Item	s	Bookmarked Items: 0	Spreadsheets:	27										
Total File Items:	5000	Bad Extension: 112	Databases:	0										
checked items:	0	Encrypted Files: 1	Graphics:	1664										
Inchecked Items	5000	From E-mail: 0	Multimedia:	0										
lagged Thumbna		Deleted Files: 2726	E-mail Messages:	0										
ther Thumbnails		From Recycle Bin: 0	Executables:	0										
ittered In:	5000	Duplicate Items: 790	Archives:	46			-	- day						
ittered Out	0	OLE Subitems: 541	Folders:	26	and the owner where the party of the local division of the local d				Cont.					
	Filtered	Flagged Ignore: 0	Slack/Free Space		and the second second	10-00		-						
	tual Files	KFF Ignorable: 0				Contraction of	Call -		-					
All items Ac	tual Files	Data Carved Files: 0	Other Known Type:	1411	ABORT THE	3 - John								
	A STREET					11								
	🍖 🗟	D 💱 off Unfiltered	~		umns	~ D12	z							
a dealership in the	🍖 📑	D 😳 OFF Unfiltered	~	All Col	umns Recycle Bi		z File Type	Category	Subject	Cr Date	Mod Date	Acc Date	L-Size	
File Name		Full Path	√		Recycle Bi	Ext F			Subject	Cr Date 11/10/2018 4:37:55 PM		Acc Date 11/10/2018 4:37:55 PM	L-Size 8,135,16	
File Name	P9	Full Path Hdd image1\Par		S\\$RECYC	Recycle Bi	Ext F	File Type		Subject		9/30/2018 2:51:32 AM		and the second sec	1
File Name	Pg	Full Path Hdd image1\Part Hdd image1\Part	_1\Bhargav Hdd-NT	S\\$RECYC	Recycle Bi	Ext F jpg Ji jpg Ji	File Type PEG/JFIF File	Graphic Graphic	Subject	11/10/2018 4:37:55 PM	9/30/2018 2:51:32 AM 9/30/2018 2:46:12 AM	11/10/2018 4:37:55 PM	8,135,16	1
File Name	Pg 99	Full Path Hdd image1\Part Hdd image1\Part Hdd image1\Part	_1\Bhargav Hdd-NTi _1\Bhargav Hdd-NTi	SISRECYC SISRECYC SISRECYC	Recycle Bi	Ext F jpg Ji jpg Ji jpg Ji	File Type PEG/JFIF File PEG/JFIF File	Graphic Graphic Graphic	Subject	11/10/2018 4:37:55 PM 11/10/2018 4:37:56 PM 11/10/2018 4:37:56 PM	9/30/2018 2:51:32 AM 9/30/2018 2:46:12 AM	11/10/2018 4:37:55 PM 11/10/2018 4:37:56 PM	8,135,16	9
File Name Travel 17.jp Travel 18.jp Travel 19.jp Travel 19.jp Travel 2.jp	99 99 99	Full Path Hdd image1\Part Hdd image1\Part Hdd image1\Part Hdd image1\Part	_1\Bhargav Hdd-NTI _1\Bhargav Hdd-NTI _1\Bhargav Hdd-NTI	SISRECYC SISRECYC SISRECYC SISRECYC	Recycle Bi	Ext F jpg Ji jpg Ji jpg Ji jpg Ji	File Type PEG/JFIF File PEG/JFIF File PEG/JFIF File	Graphic Graphic Graphic Graphic	Subject	11/10/2018 4:37:55 PM 11/10/2018 4:37:56 PM 11/10/2018 4:37:56 PM 11/10/2018 4:37:56 PM 11/10/2018 4:37:56 PM	9/30/2018 2:51:32 AM 9/30/2018 2:46:12 AM 9/30/2018 2:51:16 AM 9/30/2018 2:45:34 AM	11/10/2018 4:37:55 PM 11/10/2018 4:37:56 PM 11/10/2018 4:37:56 PM	8,135,16 3,672,12 7,680,26	1 9 5 3
File Name travel 17.jn travel 18.jn travel 19.jn travel 2.jp travel 2.jp	99 99 99 99 99	Full Path Hdd image1\Part Hdd image1\Part Hdd image1\Part Hdd image1\Part Hdd image1\Part	_1\Bhargav Hdd-NTi _1\Bhargav Hdd-NTi _1\Bhargav Hdd-NTi _1\Bhargav Hdd-NTi _1\Bhargav Hdd-NTi	SISRECYC SISRECYC SISRECYC SISRECYC SISRECYC	Recycle Bi	Ext F jpg JI jpg JI jpg JI jpg JI	File Type PEG/JFIF File PEG/JFIF File PEG/JFIF File PEG/JFIF File	Graphic Graphic Graphic Graphic Graphic	Subject	11/10/2018 4:37:55 PM 11/10/2018 4:37:56 PM 11/10/2018 4:37:56 PM 11/10/2018 4:37:56 PM 11/10/2018 4:37:56 PM	9/30/2018 2:51:32 AM 9/30/2018 2:46:12 AM 9/30/2018 2:51:16 AM 9/30/2018 2:45:34 AM 9/29/2018 2:33:02 PM	11/10/2018 4:37:55 PM 11/10/2018 4:37:56 PM 11/10/2018 4:37:56 PM 11/10/2018 4:37:56 PM 11/10/2018 4:37:56 PM	8,135,16 3,672,121 7,680,269 2,135,48 5,57 11,235	1 9 5 3 1 9
File Name Travel 17.ji Travel 18.ji Travel 19.ji Travel 2.jp Travel 2.jp Travel 21.ji Travel 21.ji	PG PG PG PG	Full Path Hdd image1/Part Hdd image1/Part Hdd image1/Part Hdd image1/Part Hdd image1/Part	1\Bhargav Hdd-NTI 1\Bhargav Hdd-NTI 1\Bhargav Hdd-NTI 1\Bhargav Hdd-NTI 1\Bhargav Hdd-NTI 1\Bhargav Hdd-NTI	SISRECYC SISRECYC SISRECYC SISRECYC SISRECYC SISRECYC	Recycle Bi	Ext F jpg JI jpg JI jpg JI jpg JI jpg JI jpg JI	File Type PEG/JFIF File PEG/JFIF File PEG/JFIF File PEG/JFIF File	Graphic Graphic Graphic Graphic Graphic Graphic	Subject	11/10/2018 4:37:55 PM 11/10/2018 4:37:56 PM 11/10/2018 4:37:56 PM 11/10/2018 4:37:56 PM 11/10/2018 4:37:56 PM	9/30/2018 2:51:32 AM 9/30/2018 2:46:12 AM 9/30/2018 2:51:16 AM 9/30/2018 2:45:34 AM 9/29/2018 2:33:02 FM 9/29/2018 2:42:26 FM	11/10/2018 4:37:55 PM 11/10/2018 4:37:56 PM 11/10/2018 4:37:56 PM 11/10/2018 4:37:56 PM 11/10/2018 4:37:56 PM	8,135,16 3,672,129 7,680,269 2,135,483 5,57	1 9 5 3 1 9
File Name travel 17.jn travel 18.jn travel 19.jn travel 2.jp travel 2.jp travel 21.jn travel 21.jn travel 21.jn	PG PG PG PG PG PG	Full Path Hdd image1Pari Hdd image1Pari Hdd image1Pari Hdd image1Pari Hdd image1Pari Hdd image1Pari	1\Bhargav Hdd-NTi 1\Bhargav Hdd-NTi 1\Bhargav Hdd-NTi 1\Bhargav Hdd-NTi 1\Bhargav Hdd-NTi 1\Bhargav Hdd-NTi	SISRECYC SISRECYC SISRECYC SISRECYC SISRECYC SISRECYC SISRECYC	Recycle Bi	Ext F jpg JI jpg JI jpg JI jpg JI jpg JI jpg JI jpg JI	File Type PEG/JFIF File PEG/JFIF File PEG/JFIF File PEG/JFIF File PEG/JFIF File PEG/JFIF File	Graphic Graphic Graphic Graphic Graphic Graphic	Subject	11/10/2018 4:37:55 PM 11/10/2018 4:37:56 PM 11/10/2018 4:37:56 PM 11/10/2018 4:37:56 PM 11/10/2018 4:37:56 PM 11/10/2018 4:37:56 PM	9/30/2018 2:51:32 AM 9/30/2018 2:45:12 AM 9/30/2018 2:45:12 AM 9/30/2018 2:51:16 AM 9/30/2018 2:45:34 AM 9/29/2018 2:33:02 PM 9/29/2018 2:42:26 PM 9/30/2018 2:52:00 AM	11/10/2018 4:37:55 PM 11/10/2018 4:37:56 PM 11/10/2018 4:37:56 PM 11/10/2018 4:37:56 PM 11/10/2018 4:37:56 PM 11/10/2018 4:37:56 PM	8,135,16 3,672,121 7,680,269 2,135,48 5,57 11,235	1 9 5 3 1 9 8
File Name	Pg Pg Pg Pg Pg Pg Pg Pg	Full Path Hdd image 1/Part Hdd image 1/Part Hdd image 1/Part Hdd image 1/Part Hdd image 1/Part Hdd image 1/Part Hdd image 1/Part	_1\Bhargav Hdd-NTI _1\Bhargav Hdd-NTI _1\Bhargav Hdd-NTI _1\Bhargav Hdd-NTI _1\Bhargav Hdd-NTI _1\Bhargav Hdd-NTI _1\Bhargav Hdd-NTI	SISRECYC SISRECYC SISRECYC SISRECYC SISRECYC SISRECYC SISRECYC SISRECYC	Recycle Bi	Ext F jpg JI jpg JI jpg JI jpg JI jpg JI jpg JI jpg JI jpg JI	File Type PEG/JFIF File PEG/JFIF File PEG/JFIF File PEG/JFIF File PEG/JFIF File PEG/JFIF File	Graphic Graphic Graphic Graphic Graphic Graphic Graphic	Subject	11/10/2018 4:37:55 PM 11/10/2018 4:37:56 PM 11/10/2018 4:37:56 PM 11/10/2018 4:37:56 PM 11/10/2018 4:37:56 PM 11/10/2018 4:37:56 PM 11/10/2018 4:37:56 PM	9/30/2018 2:51:32 AM 9/30/2018 2:45:12 AM 9/30/2018 2:51:16 AM 9/30/2018 2:45:34 AM 9/29/2018 2:33:02 PM 9/29/2018 2:42:26 PM 9/30/2018 2:42:26 AM	11/10/2018 4:37:55 PM 11/10/2018 4:37:56 PM 11/10/2018 4:37:56 PM 11/10/2018 4:37:56 PM 11/10/2018 4:37:56 PM 11/10/2018 4:37:56 PM 11/10/2018 4:37:56 PM	8,135,16 3,672,121 7,680,261 2,135,48 2,680,771 11,231 2,660,771 909,371 2,331,250	1 9 5 3 1 9 8 9 8
File Name	Pg Pg Pg Pg Pg Pg Pg Pg Pg Pg	Full Path Hdd image 1/Part Hdd image 1/Part	1\Bhargav Hdd-NTi 1\Bhargav Hdd-NTi 1\Bhargav Hdd-NTi 1\Bhargav Hdd-NTi _1\Bhargav Hdd-NTi 1\Bhargav Hdd-NTi _1\Bhargav Hdd-NTi _1\Bhargav Hdd-NTi	SISRECYC SISRECYC SISRECYC SISRECYC SISRECYC SISRECYC SISRECYC SISRECYC SISRECYC	Recycle Bi	Ext F jpg JI jpg JI jpg JI jpg JI jpg JI jpg JI jpg JI jpg JI jpg JI	File Type PEG/JFIF File PEG/JFIF File PEG/JFIF File PEG/JFIF File PEG/JFIF File PEG/JFIF File	Graphic Graphic Graphic Graphic Graphic Graphic Graphic Graphic	Subject	11/10/2018 4:37:55 PM 11/10/2018 4:37:56 PM 11/10/2018 4:37:56 PM 11/10/2018 4:37:56 PM 11/10/2018 4:37:56 PM 11/10/2018 4:37:56 PM 11/10/2018 4:37:56 PM	9/30/2018 2:51:32 AM 9/30/2018 2:46:12 AM 9/30/2018 2:61:16 AM 9/30/2018 2:51:16 AM 9/30/2018 2:46:34 AM 9/29/2018 2:46:34 AM 9/30/2018 2:42:26 PM 9/30/2018 2:42:26 PM 9/30/2018 2:42:00 AM	11/10/2018 4:37:55 PM 11/10/2018 4:37:56 PM 11/10/2018 4:37:56 PM 11/10/2018 4:37:56 PM 11/10/2018 4:37:56 PM 11/10/2018 4:37:56 PM 11/10/2018 4:37:56 PM	8,135,16 3,672,121 7,680,261 2,136,481 5,57 11,231 2,660,771 909,371 2,331,251 146,432	1 9 5 3 1 9 8 9 8 9 8 9
File Name           If File Name           If travel 17.jrj           If travel 18.jrj           If travel 19.jrj           If travel 2.jrj           I	Pg Pg Pg Pg Pg Pg Pg Pg Pg Pg	Full Path Hidd image 1Pan Hidd image 1Pan	1\Bhargav Hdd-NTI 1\Bhargav Hdd-NTI 1\Bhargav Hdd-NTI 1\Bhargav Hdd-NTI <b>1\Bhargav Hdd-NTI</b> 1\Bhargav Hdd-NTI 1\Bhargav Hdd-NTI 1\Bhargav Hdd-NTI 1\Bhargav Hdd-NTI	SISRECYC SISRECYC SISRECYC SISRECYC SISRECYC SISRECYC SISRECYC SISRECYC SISRECYC SISRECYC SISRECYC	Recycle Bi	Ext F jpg JI jpg JI jpg JI jpg JI jpg JI jpg JI jpg JI doc N	File Type PEG/JFIF File PEG/JFIF File PEG/JFIF File PEG/JFIF File PEG/JFIF File PEG/JFIF File PEG/JFIF File	Graphic Graphic Graphic Graphic Graphic Graphic Graphic Graphic Graphic Graphic Document	Subject	11/10/2018 4:37:55 PM 11/10/2018 4:37:56 PM	9/30/2018 2:51:32 AM 9/30/2018 2:46:12 AM 9/30/2018 2:61:16 AM 9/30/2018 2:46:34 AM 9/29/2018 2:46:34 AM 9/29/2018 2:42:26 PM 9/30/2018 2:52:00 AM 9/30/2018 2:42:00 AM 9/30/2018 2:42:10 AM 10/1/2018 2:08:28 AM	11/10/2018 4:37:55 PM 11/10/2018 4:37:56 PM	8,135,16 3,672,121 7,680,261 2,135,48 2,680,771 11,231 2,660,771 909,371 2,331,250	1 9 5 3 1 9 8 9 8 9 8 9
File Name           If travel 17. ji           If travel 18. ji           If travel 19. ji           If travel 2. ji           If travel 2.1 ji           If travel 2.1 ji           If travel 2.1 ji           If travel 2.1 ji           If travel 2.2 ji           If travel 2.3 ji           If travel 2.4 ji           If travel 2.4 ji           If travel 2.4 ji           If travel 2.4 ji           If travel 2.6 ji	000 000 000 000 000 000 000 000 000 00	Full Path Hdd image11Pat Hdd image11Pat Hdd image11Pat Hdd image11Pat Hdd image11Pat Hdd image11Pat Hdd image11Pat Hdd image11Pat Hdd image11Pat	1\Bhargav Hdd-NT1 1\Bhargav Hdd-NT1 1\Bhargav Hdd-NT1 1\Bhargav Hdd-NT1 1\Bhargav Hdd-NT1 1\Bhargav Hdd-NT1 1\Bhargav Hdd-NT1 1\Bhargav Hdd-NT1 1\Bhargav Hdd-NT1 1\Bhargav Hdd-NT1	SISRECYC SISRECYC SISRECYC SISRECYC SISRECYC SISRECYC SISRECYC SISRECYC SISRECYC SISRECYC SISRECYC SISRECYC SISRECYC	Recycle Bi	Ext F jpg J jpg J jpg J jpg J jpg J jpg J jpg J jpg J jpg J doc N doc N jpg J	File Type PEG/JFIF File PEG/JFIF File PEG/JFIF File PEG/JFIF File PEG/JFIF File PEG/JFIF File PEG/JFIF File Iiarosoft Wor PEG/JFIF File	Graphic Graphic Graphic Graphic Graphic Graphic Graphic Graphic Graphic Graphic Document	Subject	11/10/2018 4:37:55 PM 11/10/2018 4:37:56 PM	9/30/2018 2:51:32 AM 9/30/2018 2:45:16 AM 9/30/2018 2:45:16 AM 9/30/2018 2:45:34 AM 9/29/2018 2:45:34 AM 9/29/2018 2:42:26 PM 9/30/2018 2:42:06 AM 9/30/2018 2:42:06 AM 9/30/2018 2:42:06 AM 9/30/2018 2:42:06 AM	11/10/2018 4:37:55 PM 11/10/2018 4:37:56 PM	8,135,16 3,672,121 7,680,261 2,136,481 5,57 11,231 2,660,771 909,371 2,331,251 146,432	1 9 5 3 1 9 8 9 8 9 8 9 8 2 0
File Name           Image: travel 17.ji           Image: travel 18.ji           Image: travel 19.ji           Image: travel 2.ji           Image: travel 22.ji           Image: travel 23.ji           Image: travel 28.di           Image: travel 28.di           Image: travel 28.di           Image: travel 3.ji           Image: travel	2000 2000 2000 2000 2000 2000 2000 200	Full Path Hdd imaget IPar Hdd imaget IPar	_1\Bhargav Hdd-NTI _1\Bhargav Hdd-NTI _1\Bhargav Hdd-NTI _1\Bhargav Hdd-NTI _1\Bhargav Hdd-NTI _1\Bhargav Hdd-NTI _1\Bhargav Hdd-NTI _1\Bhargav Hdd-NTI _1\Bhargav Hdd-NTI _1\Bhargav Hdd-NTI	SISRECYC SISRECYC SISRECYC SISRECYC SISRECYC SISRECYC SISRECYC SISRECYC SISRECYC SISRECYC SISRECYC SISRECYC SISRECYC	Recycle Bi har har har har har har har har	Ext F jpg J jpg J jpg J jpg J jpg J jpg J jpg J jpg J jpg J doc N doc N jpg J	File Type PEG/JFIF File PEG/JFIF File PEG/JFIF File PEG/JFIF File PEG/JFIF File PEG/JFIF File PEG/JFIF File Itirosoft Wor	Graphic Graphic Graphic Graphic Graphic Graphic Graphic Graphic Graphic Document Document	Subject	11/10/2018 4:37:55 PM 11/10/2018 4:37:56 PM	9/30/2018 2:51:32 AM 9/30/2018 2:45:12 AM 9/30/2018 2:45:116 AM 9/30/2018 2:45:30 CF PM 9/30/2018 2:45:30 CF PM 9/30/2018 2:42:20 FM 9/30/2018 2:42:20 AM 9/30/2018 2:42:20 AM 10/1/2018 2:36:22 AM 10/1/2018 2:36:22 AA	11/10/2018 4:37:56 PM 11/10/2018 4:37:56 PM	8,135,16 3,672,121 7,680,261 2,136,481 <b>5,57</b> 11,231 2,660,771 909,371 2,331,251 146,432 79,360	1 9 5 3 1 9 8 9 8 9 8 9 8 2 0 8
File Name           Image: travel 17.ji           Image: travel 18.ji           Image: travel 19.ji           Image: travel 2.ji           Image: travel 22.ji           Image: travel 23.ji           Image: travel 28.di           Image: travel 28.di           Image: travel 28.di           Image: travel 3.ji           Image: travel	2000 2000 2000 2000 2000 2000 2000 200	Full Path Hdd image11Par Hdd image11Par	18hargav Hdd-NTI _18hargav Hdd-NTI	SISRECYC SISRECYC SISRECYC SISRECYC SISRECYC SISRECYC SISRECYC SISRECYC SISRECYC SISRECYC SISRECYC SISRECYC SISRECYC	Recycle Bi here her	Ext F jpg J jpg J jpg J jpg J jpg J jpg J jpg J jpg J doc N doc N jpg J jpg J jp	File Type PEG/JFIF File PEG/JFIF File PEG/JFIF File PEG/JFIF File PEG/JFIF File PEG/JFIF File PEG/JFIF File Iiarosoft Wor PEG/JFIF File	Graphic Graphic Graphic Graphic Graphic Graphic Graphic Graphic Document Document Graphic Graphic Graphic Graphic	Subject	11/10/2018 4:37:56 PM 11/10/2018 4:37:56 PM	9/30/2018 2:51:32 AM 9/30/2018 2:45:16 AM 9/30/2018 2:45:16 AM 9/20/2018 2:45:34 AM 9/29/2018 2:45:34 AM 9/29/2018 2:42:26 PM 9/30/2018 2:42:26 PM 9/30/2018 2:42:06 AM 9/30/2018 2:42:06 AM 9/30/2018 2:45:26 AM 9/30/2018 2:45:26 AM	11/10/2018 4:37:56 PM 11/10/2018 4:37:56 PM	8,135,16 3,672,121 7,680,261 2,135,481 5,57 11,231 2,660,771 909,371 2,331,261 148,433 79,361 1,073,821	1 9 5 3 9 8 9 8 9 8 9 8 9 8 2 0 8 5
File Name           Image: seven 17.ji           <	2000 2000 2000 2000 2000 2000 2000 200	Full Path Hdd image1 Part Hdd image1 Part		SISRECYC SISRECYC SISRECYC SISRECYC SISRECYC SISRECYC SISRECYC SISRECYC SISRECYC SISRECYC SISRECYC SISRECYC SISRECYC SISRECYC	Recycle Bi are are are are are are are are	Ext F jpg J jpg J jpg J jpg J jpg J jpg J jpg J doc N doc N jpg J jpg J jp	File Type PEG/JFIF File PEG/JFIF File PEG/JFIF File PEG/JFIF File PEG/JFIF File PEG/JFIF File PEG/JFIF File PEG/JFIF File PEG/JFIF File	Graphic Graphic Graphic Graphic Graphic Graphic Graphic Graphic Document Document Graphic Graphic Graphic Graphic Graphic Graphic	Subject	11/10/2018 4:37:65 PM 11/10/2018 4:37:65 PM	9/30/2018 2:51:32 AM 9/30/2018 2:46:12 AM 9/30/2018 2:51:16 AM 9/30/2018 2:51:16 AM 9/30/2018 2:45:34 AM 9/30/2018 2:45:24 AM 9/30/2018 2:42:20 AM 9/30/2018 2:42:20 AM 9/30/2018 2:45:06 AM 9/30/2018 2:45:84 AM 9/30/2018 2:46:85 AM 9/30/2018 2:46:86 AM	11/10/2018 4:37:56 PM 11/10/2018 4:37:56 PM	8,136,16' 3,672,121 7,680,264 2,136,48 2,136,48 2,680,774 909,371 2,331,261 146,43 79,360 1,073,821 4,848,385	1 9 5 3 1 9 8 9 8 2 0 8 7
File Name File N	2000 2000 2000 2000 2000 2000 2000 200	Full Path Hdd image1Par Hdd image1Par		SISRECYC SISRECYC SISRECYC SISRECYC SISRECYC SISRECYC SISRECYC SISRECYC SISRECYC SISRECYC SISRECYC SISRECYC SISRECYC SISRECYC SISRECYC SISRECYC SISRECYC	Recycle Bi           Kara           Kara<	Ext F jpg J jpg J jpg J jpg J jpg J jpg J jpg J jpg J doc N doc N jpg J jpg J jp	File Type PEG/JFIF File PEG/JFIF File PEG/JFIF File PEG/JFIF File PEG/JFIF File PEG/JFIF File PEG/JFIF File PEG/JFIF File PEG/JFIF File PEG/JFIF File	Graphic Graphic Graphic Graphic Graphic Graphic Graphic Graphic Document Document Graphic Graphic Graphic Graphic Graphic Graphic	Subject	11/10/2018 4:37:56 PM 11/10/2018 4:37:56 PM	9/30/2018 2:51.52 AM 9/30/2018 2:45.12 AM 9/30/2018 2:45.116 AM 9/30/2018 2:45.116 AM 9/30/2018 2:45.30 AP 9/30/2018 2:45.20 AM 9/30/2018 2:45.20 AM 9/30/2018 2:45.20 AM 9/30/2018 2:45.20 AM 10/1/2018 2:55.42 AM 9/30/2018 2:44.52 AM 9/30/2018 2:44.52 AM	11/10/2018 4:37:56 PM 11/10/2018 4:37:56 PM	8,138,16 3,672,121 7,680,264 2,138,48 2,680,771 909,371 2,331,264 146,431 79,360 1,073,821 4,848,388 9,202,411	1 9 5 3 1 9 8 9 8 9 8 2 0 8 5 7 6

Figure 85. Image Preview 3 for HDD Image

When we click on one of the excel files, we can recover it, and we can see the preview of

the excel as follows.

File Status           KFF Alert Files:         0           Bookmarked Items:         0           Bad Extension:         112	File Category Documents: 1449 Spreadsheets: 27 Databases: 0	<b>"</b>	!	• <b>,</b> ₩ ₩	क्ये क्ये 😣	D 🔊					
Bookmarked Items: 0 Bad Extension: 112	Spreadsheets: 27		A	A COLORED OF THE OWNER	ital (ital)						
Bad Extension: 112			A		C	7	D		F	1 7	F
	Databases: 0		Ormaniastic		Culture	A					
	Uninerated. U	1	Organisatio	hal Safet	Culture	Appraisal t	ool data analysis	spreadsheet			
Encrypted Files: 1	Graphics: 1664	2									
From E-mail: 0	Multimedia: 0	3	Instructions	for using	this spre	adsheet					
Deleted Files: 2726	E-mail Messages: 0	4	1. Complete det	tails of safet	y culture ap	praisal below -	a new spreadsheet sh	nould be used for eac	ch appraisal		
From Recycle Bin: 0	Executables: 0	5	2. Take your co	mpleted sc	nario data e	ntry sheets ar	nd choose which scena	and to enter first			
Duplicate Items: 790	Archives: 46	6	3. Select the co	rresponding	scenario wo	orksheet (usin	g tabs or click on hype	erlink below)			
OLE Subitems: 541	Folders: 26	7									
Flagged Ignore: 0	Slack/Free Space: 182	8									
KFF Ignorable: 0	Other Known Type: 195	9	Note: that the n	umbers will	not be in ord						
Data Carved Files: 0	Unknown Type: 1411		Front Pa	ge / Scenari	1 / Scenario	i <	information		6 -1 1 #6	!! 6!!.	>
	Deleted Files:         2726           From Recycle Bin:         0           Duplicate items:         790           OLE Subitems:         541           Flagged ignore:         0           KFF ignorable:         0	Deleted Files:         2726         E-mail Messages:         0           From Recycle Bin:         0         Executables:         0           Duplicate terms:         790         Archives:         46           OLE Stubberns:         541         Folders:         28           Flagped Ignore:         0         Slack/Free Space:         182           KFF Ignorable:         0         Unknown Type:         191	Deleted Files:         2726         E-mail Messages:         0         4           From Recycle Bin:         0         Executables:         0         5           Duplicate Terms:         790         Archives:         46         6           OLE Subhems:         541         Folders:         26         7           Flagged Ignore:         0         Stact/Free Space:         182         9           VER Fignorable:         0         Unknown Type:         195         9           Data Carved Files:         0         Unknown Type:         141         411	Deleted Files:         2726         E-mail Messages:         0         4         1. Complete del 5         2. Take your co           Duplicate tems:         790         Archives:         46         6         3. Select the co           Duplicate tems:         790         Archives:         46         6         3. Select the co           Diplicate tems:         790         Archives:         46         6         3. Select the co           Diplicate tems:         701         Folders:         28         7         4. Enter the ref           Flagped tynore:         0         Stack/Free Space:         18         8         5. Transfer your           VFF tynorable:         0         Unknown Type:         141         141         4	Deleted Files         2726         E-mail Messages:         0         4         1. Complete details of safet           From Recycle Bin:         0         Executables:         0         5         2. Take your completed sci.           Duplicate terms:         794         Archives:         46         6         3. Select the corresponding           OLE Subtems:         541         Folders:         26         7         4. Enter the reference num           Flagped Ignore:         0         Slack/Free Space:         182         8         5. Transfer your instrings fron           Physics         0         Other Known Type:         1411         14         14	Deleted Files:     2726     E-mail Messages:     0     4     1. Complete details of safety culture applement of the culture applement	Deleted Files:     2726     E-mail Messages:     0       From Recycle Bin:     0     Executables:     0       Southerms:     790     Archives:     4       Duplicate terms:     790     Archives:     46       Subtema:     541     Forders:     28       Flagped tynore:     0     Stack/Free Space:     12       Stack/Free Space:     10     51     Fransfer your ratings from the data collection sheet       9     Note: that the numbers will not be in order: However this       9     Note: that the numbers will not be in order: However this       14     1. Complete details of safety culture appraisal below-       52     7.4     Enter the reference number for the index collection sheet       9     Note: that the numbers will not be in order: However this       14     1. Complete details of safety culture appraisal below-	Deleted Files.       2726       E-mail Messages:       0       4       1. Complete defails of safety culture appraisal below - a new spreadsheet sit         From Recycle Bin:       0       Executables:       0       5       2. Take your completed scenario data entry sheets and choose which scenario         Duplicate terms:       794       Archives:       46       6       3. Select the corresponding scenario worksheet (using tabs or click on hype         OLE Subtems:       541       Folders:       26       7       4. Enter the reference number for the interviewe whose data you are entering         Flagped ignore:       0       Slack/Free Space:       182       8       5. Transfer your rainings from the data collection sheet into the relevant work:         9       Note: that the numbers will not be in order. However the data entry sheet foll       9       Note: that the numbers will not be in order. However the data entry sheet foll         VFF giorable:       0       Unknown Type:       1411       Yer Provider Scenario 1, Scenario 1, Scenario 1, Scenario 1, Scenario 1, Scenario 2, C	Deleted Fies.       2726       E-mail Messages:       0       4       1. Complete defails of safety culture appraisal below - a new spreadsheet should be used for east from Recycle Bin:         Deleted Fies.       0       Executables:       0       5       2. Take your completed scinario data entry sheets and choose which scenario to enter first Dupletate terms:         Dupletate terms:       794       Folders:       7       4. Enter the reference number for the inference whose data you are entering         Flagped ignore:       0       Stack/Free Space:       182       8       5. Transfer your tarings from the data collection sheet into the relevant worksheet (user) whose data entry sheet follow the order of the informations of the information of t	Deleted Fies     2726     E-mail Messages:     0       From Recycle Bin:     0     Executables:     0       Diplicate Terms:     794     A function of the second o	Deleted Files         2726         E-mail Messages:         0         4         1. Complete details of safety culture appraisal below - a new spreadsheet should be used for each appraisal           From Recycle Bin:         0         Executables:         0         5         2. Take your completed scenario data entry sheets and choose which scenario to enter first         0           Duplicate terms:         790         Archives:         46         6         3. Select the corresponding scenario worksheet (using tabs or cick on hyperink below)         0           OLE Subtems:         51         Folders:         28         7         4. Enter the reference number for the inferievee whose data you are entering         1           Flagped ignore:         0         Siack/Free Space:         162         8. 5. Transfer your raining, form the data collection         9         Note: that the numbers will not be in order. However the data entry sheet follow the order of the interview questions and support of the interview question

*Figure 86*. Excel Preview for HDD Image

When we click on one of the document files, we can recover it, and we can see the

preview of the document as follows.

73

Image: Part Teber and Hod image 1Part Teberage Hed-HTFSIGRECYC         xml         XML         Document         NA         1//1980 120000AM         NA         2.2           Image: Image 1Part Teberage Hed-HTFSIGRECYC         xml         XML         Document         NA         1//1980 120000AM         NA         2.3           Image: Image 1Part Teberage Hed-HTFSIGRECYC         xml         XML         Document         NA         1//1980 120000AM         NA         2.5           Image: Image 1Part Teberage Hed-HTFSIGRECYC         xml         XML         Document         NA         1//1980 120000AM         NA         2.5           Image: Image 1Part Teberage Hed-HTFSIGRECYC         xml         XML         Document         NA         1//1980 120000AM         NA         2.5           Image: Image 1Part Teberage Hed-HTFSIGRECYC         xml         XML         Document         NA         1//1980 120000AM         NA         2.2           Image: Image 1Part Teberage Hed-HTFSIGRECYC         xml         XML         Document         NA         1//1980 120000AM         NA         2.2           Image: Image 1Part Teberage Hed-HTFSIGRECYC         xml         XML         Document         NA         1//1980 120000AM         NA         2.2           Image: Image 1Part TeBrage Hed-HTFSI	Overview	Explor	re Graphics	E-Mail Search	Bookm	ark								
vidence tems: 2   KFF Alert Files: 0   Documents: 1448] File Name Bookmatcel tems: 0   Detected Files: 272 bereakbets: 0   Detected Files: 0   Unknown Type: 195 Beta Cancer Files: 0   Unknown Type: 1	Evidence Item	8	File Status	File Category	<b>n</b>	~ A	<b>20</b>	ම බබ 👩 👩	ñ 🔊					
tal File terms 5000 Fierd Files 5000 Fine Recycle Files 5000 Fine Recycle Bin 5000 Fine Recycle Bin 50000 Fine Recy	vidence Items:	2	KFF Alert Files: 0	Documents: 1449	•		·    · · · <b>↓</b>							
hecked tems: 000 PromE-maik 0	File Items		Bookmarked Items: 0	Spreadsheets: 27	1									
nchecked tema: 500 gaged Thumbnais: 0 terred In: 5000 Dupicate tems. 790 Archives: 461 Form E-mail Messages: 0 Archives: 461 Form E-mail Messages: 0 Archives: 461 Form E-mail Messages: 0 Dupicate tems. 790 Archives: 461 Form E-mail Messages: 0 Dupicate tems. 790 Archives: 461 Form E-mail Messages: 0 Dupicate tems. 790 Dupicate	tal File Items:	5000	Bad Extension: 112	Databases: 0										
Baged Thumbnalis: beref htter Thumbnalis: beref htter Store Sto	hecked Items:	0	Encrypted Files: 1	Graphics: 1664										
her Thumbalis: 1664 Forder 2000 0 ELE Subtemes: 540 Duplicate terms: 750 Actual Files Actual Fi	nchecked Items:	5000	From E-mail: 0	Multimedia: 0										
Barred In:       Opplicate tens.       790       Archives:       46         In Initial Capital Letters       Fileged ignore:       0       Diskuberns:       541       Foodsets:       560         All tens       Actual Files       Sack/Free Space:       10       Disk for space:       0       Disk for space:       0         Bit	agged Thumbnails:	0	Deleted Files: 2726	E-mail Messages: 0	Title of	f For	mal D	ocume	nt					
Bared Out       OLE Subtems:       541       Folders:       26         Inflected       Fårderd       Skack/ree Space:       102         Actual Files       Actual Files       Other Known Type:       193         Imber of Space:       Ditter Known Type:       193         Imber of Space:       Full Path       Recycle Bi       Ext       File Type       Category       Subject       Cr Date       Mod Date       Acc Date       L-Size         Imbort Space:       Full Path       Recycle Bi       Ext       File Type       Category       Subject       Cr Date       Mod Date       Acc Date       L-Size         Import Space:       Space:       XML       Document       N/A       1/1/1980 12:00:00 AM       N/A       2.3         Import Space:       Space:       XML       Document       N/A       1/1/1980 12:00:00 AM       N/A       2.4         Import Space:       Space:       XML       Document       N/A       1/1/1980 12:00:00 AM       N/A       2.5         Import Space:       XML	ther Thumbnails:	1664	From Recycle Bin: 0	Executables: 0										
Bared Out       OLE Subtems:       541       Folders:       26         Inflected       Fårderd       Skack/ree Space:       102         Actual Files       Actual Files       Other Known Type:       193         Imber of Space:       Ditter Known Type:       193         Imber of Space:       Full Path       Recycle Bi       Ext       File Type       Category       Subject       Cr Date       Mod Date       Acc Date       L-Size         Imbort Space:       Full Path       Recycle Bi       Ext       File Type       Category       Subject       Cr Date       Mod Date       Acc Date       L-Size         Import Space:       Space:       XML       Document       N/A       1/1/1980 12:00:00 AM       N/A       2.3         Import Space:       Space:       XML       Document       N/A       1/1/1980 12:00:00 AM       N/A       2.4         Import Space:       Space:       XML       Document       N/A       1/1/1980 12:00:00 AM       N/A       2.5         Import Space:       XML	tered In:	5000	Duplicate Items: 790	Archives: 46	in Initia	al Ca	pital L	etters.						
Initiates         Flaged lynore:         0         Siack/Free Space:         182           At terms         Actual Files         KFF ignorable:         0         Other Known Type:         195           At terms         Actual Files         KFF ignorable:         0         Other Known Type:         195           Image: The Stack Press:         0         Image: The Stack Press:         0         Image: The Stack Press:         0           Image: The Stack Press:         0         Image: The Stack Press:         0         Image: The Stack Press:         0           Image: The Stack Press:         0         Image: The Stack Press:         0         Image: The Stack Press:         0           Image: The Stack Press:         0         Image: The Stack Press:         0         Image: The Stack Press:         0           Image: The Stack Press:         0         Image: The Stack Press:         0         Image: The Stack Press:         0           Image: The Stack Press:         0         Image: The Stack Press:         0         Image: The Stack Press:         0           Image: The Stack Press:         0         Image: The Stack Press:         0         Image: The Stack Press:         0           Image: The Stack Press:         0         Image: The Stack Press:         0	itered Out:	0					•							
Al tem Actual Files Actual File	Infiltered Filte	ered	Flagged Ignore: 0	Slack/Free Space: 182										
Data Carved Files:       Unknown Type:       1411         Coll       Dista Carved Files:       Unknown Type:       1411         File Name       Full Path       Recycle Bi       Ext.       File Type       Category       Subject       Cr Date       Mod Date       Acc Date       L-Size         Image:       Full Path       Recycle Bi       Ext.       File Type       Category       Subject       Cr Date       Mod Date       Acc Date       L-Size         Image:       Full Path       Hed image:       File:       Type       Category       Subject       Cr Date       Mod Date       Acc Date       L-Size         Image:       Full Path       Hed image:       File:       Type       Category       Subject       Cr Date       Mod Date       Acc Date       L-Size         Image:       Full Path       Hed image:       Hed.       Tissies:       NAL       Document       N/A       1///1980 12:00:00 AM       N/A       2.2         Image:       Full Path:       Heagar Heart:       Heagar Heart       N/A       Document       N/A       1///1980 12:00:00 AM       N/A       2.2         Image:       Full Path:       Heagar Heart       Heagar Head       Head Heage:       Head Heage:	All Items Actua	Files												
Bit of the second part of the second pa			-		<									
Image Name         Hed Image Name				V All Colu				Category	Subject	CrDate	Mod Date	Acc Date	L-Size	
EndTable.xml         Hdd image1Part_1Bhargav Hdd4TFSISRECYC         xml         XML         Document         NA         1/1/1980 120:00 AM         NA         2.25           fontTable.xml         Hdd image1Part_1Bhargav Hdd4TFSISRECYC         xml         XML         Document         NA         1/1/1980 120:00 AM         NA         3.3           fontTable.xml         Hdd image1Part_1Bhargav Hdd4TFSISRECYC         xml         XML         Document         NA         1/1/1980 120:00 AM         NA         3.4           fontTable.xml         Hdd image1Part_1Bhargav Hdd4TFSISRECYC         xml         XML         Document         NA         1/1/1980 120:00 AM         NA         2.2           fontTable.xml         Hdd image1Part_1Bhargav Hdd4TFSISRECYC         xml         XML         Document         NA         1/1/1980 120:00 AM         NA         2.2           fontTable.xml         Hdd image1Part_1Bhargav Hdd4TFSISRECYC         xml         XML         Document         NA         1/1/1980 120:00 AM         NA         2.2           fontTable.xml         Hdd image1Part_1Bhargav Hdd4TFSISRECYC         xml         XML         Document         NA         1/1/1980 120:00 AM         NA         1.2           fontTable.xml etail         Hdd image1Part_1Bhargav Hdd4TFSISRECYC         xml	File Name		Full Path Hdd image1\Par	_1\Bhargav Hdd-NTFS\\$RECYC	Recycle Bi	Ext F xml X	ile Type ML	Document	Subject	N/A	1/1/1980 12:00:00 AM	N/A	3,823	
Image Name         Hed Image Name         Hed Image Name         Hed Image Name         Nam         Name <td>File Name fontTable.xm</td> <td>   </td> <td>Full Path Hdd image1\Part Hdd image1\Part</td> <td>_1\Bhargav Hdd-NTFS\\$RECYC _1\Bhargav Hdd-NTFS\\$RECYC</td> <td>Recycle Bi</td> <td>Ext F xml X xml X</td> <td>ile Type ML ML</td> <td>Document Document</td> <td>Subject</td> <td>N/A N/A</td> <td>1/1/1980 12:00:00 AM 1/1/1980 12:00:00 AM</td> <td>N/A. N/A</td> <td>3,823</td> <td>7</td>	File Name fontTable.xm	 	Full Path Hdd image1\Part Hdd image1\Part	_1\Bhargav Hdd-NTFS\\$RECYC _1\Bhargav Hdd-NTFS\\$RECYC	Recycle Bi	Ext F xml X xml X	ile Type ML ML	Document Document	Subject	N/A N/A	1/1/1980 12:00:00 AM 1/1/1980 12:00:00 AM	N/A. N/A	3,823	7
Image 1Part, 19kangav Hdol.HTFS/SRECYC         xml         XML         Document         NA         1/1/1980 120000AM         NA         1.4           If fontTable.xml         Hdd image 1Part, 19kangav Hdol.HTFS/SRECYC         xml         XML         Document         NA         1/1/1980 120000AM         NA         2.5           If fontTable.xml         Hdd image 1Part, 19kangav Hdol.HTFS/SRECYC         xml         XML         Document         NA         1/1/1980 120000AM         NA         2.5           If ontTable.xml         Hdd image 1Part, 19kangav Hdol.HTFS/SRECYC         xml         XML         Document         NA         1/1/1980 120000AM         NA         2.5           If ontTable.xml         Hdd image 1Part, 19kangav Hdol.HTFS/SRECYC         xml         XML         Document         NA         1/1/1980 120000AM         NA         2.5           If ontTable.xml rels         Hdd image 1Part, 19kangav Hdol.HTFS/SRECYC         xml         XML         Document         NA         1/1/1980 120000AM         NA         1.6           If ontTable.xml rels         Hdd image 1Part, 19kangav Hdol.HTFS/SRECYC         xml         XML         Document         11/102018 437.31 PM         10/2018 437.31 PM         7.2         4.8           If ood 2.5 docx         Hdd image 1Part, 19kangav Hdol.HTFS/SRECYC	File Name fontTable.xm	-	Full Path Hdd image1\Part Hdd image1\Part Hdd image1\Part	_1\Bhargav Hdd-NTFS\\$RECYC. _1\Bhargav Hdd-NTFS\\$RECYC. _1\Bhargav Hdd-NTFS\\$RECYC.	Recycle Bi	Ext F xml X xml X xml X	File Type ML ML ML	Document Document Document	Subject	N/A N/A <b>N/A</b>	1/1/1980 12:00:00 AM 1/1/1980 12:00:00 AM 1/1/1980 12:00:00 AM	N/A N/A <b>N/A</b>	3,823 2,797 <b>3,35</b> 5	5
Image:         Image:<	File Name	- <u>   - 4</u>     	Full Path Hdd image1\Part Hdd image1\Part Hdd image1\Part Hdd image1\Part	1\Bhargav Hdd-NTFS\SRECYC 1\Bhargav Hdd-NTFS\SRECYC. 1\Bhargav Hdd-NTFS\SRECYC 1\Bhargav Hdd-NTFS\SRECYC	Recycle Bi	Ext F xml Xi xml Xi xml Xi xml Xi	File Type ML ML ML ML	Document Document Document	Subject	N/A N/A N/A	1/1/1980 12:00:00 AM 1/1/1980 12:00:00 AM 1/1/1980 12:00:00 AM 1/1/1980 12:00:00 AM	N/A N/A N/A N/A	3,823 2,797 3,355 2,983	5
Image Name         Hed Image Name         Hed Image Name         Hed Image Name         Nam         Name <td>File Name fontTable.xmi fontTable.xmi fontTable.xmi fontTable.xmi fontTable.xmi</td> <td></td> <td>Full Path Hdd image1\Path Hdd image1\Path Hdd image1\Path Hdd image1\Path Hdd image1\Path</td> <td>L18hargav Hdd-NTFS\SRECYC L18hargav Hdd-NTFS\SRECYC L18hargav Hdd-NTFS\SRECYC L18hargav Hdd-NTFS\SRECYC L18hargav Hdd-NTFS\SRECYC</td> <td>Recycle Bi</td> <td>Ext F xml Xi xml Xi xml Xi xml Xi xml Xi</td> <td>File Type ML ML ML ML ML ML</td> <td>Document Document Document Document Document</td> <td>Subject</td> <td>N/A N/A N/A N/A</td> <td>1/1/1980 12:00:00 AM 1/1/1980 12:00:00 AM 1/1/1980 12:00:00 AM 1/1/1980 12:00:00 AM 1/1/1980 12:00:00 AM</td> <td>N/A N/A N/A N/A</td> <td>3,823 2,797 3,356 2,983 3,386</td> <td>7 5 3 6</td>	File Name fontTable.xmi fontTable.xmi fontTable.xmi fontTable.xmi fontTable.xmi		Full Path Hdd image1\Path Hdd image1\Path Hdd image1\Path Hdd image1\Path Hdd image1\Path	L18hargav Hdd-NTFS\SRECYC L18hargav Hdd-NTFS\SRECYC L18hargav Hdd-NTFS\SRECYC L18hargav Hdd-NTFS\SRECYC L18hargav Hdd-NTFS\SRECYC	Recycle Bi	Ext F xml Xi xml Xi xml Xi xml Xi xml Xi	File Type ML ML ML ML ML ML	Document Document Document Document Document	Subject	N/A N/A N/A N/A	1/1/1980 12:00:00 AM 1/1/1980 12:00:00 AM 1/1/1980 12:00:00 AM 1/1/1980 12:00:00 AM 1/1/1980 12:00:00 AM	N/A N/A N/A N/A	3,823 2,797 3,356 2,983 3,386	7 5 3 6
Image 1Part_1Bhagav Hdol-NTFSISRECYC         xml         XML         Document         NA         1/1/1980 12:00:00.AM         NA         2.2.4           Image 1Part_1Bhagav Hdol-NTFSISRECYC         xml         XML         Document         NA         1/1/1980 12:00:00.AM         NA         2.4           Image 1Part_1Bhagav Hdol-NTFSISRECYC         rels         XML         Document         NA         1/1/1980 12:00:00.AM         NA         1.4           Image 1Part_1Bhagav Hdol-NTFSISRECYC         rels         XML         Document         NA         1/1/1980 12:00:00.AM         NA         1.4           Image 1Part_1Bhagav Hdol-NTFSISRECYC         docx         MC files 2.1         Document         11/10:2018 4:37:31 PM         10/12:018 4:37:31 PM         2.497.4           Image 1Part_1Bhagav Hdol-NTFSISRECYC         docx         MA         Document         NA         11/1950 12:00:00 AM         NA         2.497.4           Image 1Part_1Bhagav Hdol-NTFSISRECYC         xml         XML         Document         NA         11/1950 12:00:00 AM         NA         2.497.4           Image 1Part_1Bhagav Hdol-NTFSISRECYC         xml         XML         Document         NA         11/11550 12:00:00 AM         NA         2.497.4           Image 1Part_1Bhagav Hdol-NTFSISRECYC	File Name font Table xmi font Table xmi font Table xmi font Table xmi font Table xmi font Table xmi		Full Path Hdd image1\Part Hdd image1\Part Hdd image1\Part Hdd image1\Part Hdd image1\Part	LiBhargav Hdd-NTFS\SRECYC. LiBhargav Hdd-NTFS\SRECYC. LiBhargav Hdd-NTFS\SRECYC. LiBhargav Hdd-NTFS\SRECYC. LiBhargav Hdd-NTFS\SRECYC. LiBhargav Hdd-NTFS\SRECYC.	Recycle Bi	Ext F xml Xi xml Xi xml Xi xml Xi xml Xi xml Xi	File Type ML ML ML ML ML ML ML	Document Document Document Document Document	Subject	N/A N/A N/A N/A N/A	1/1/1980 12:00:00 AM 1/1/1980 12:00:00 AM 1/1/1980 12:00:00 AM 1/1/1980 12:00:00 AM 1/1/1980 12:00:00 AM 1/1/1980 12:00:00 AM	N/A N/A N/A N/A N/A	3,823 2,797 3,355 2,983	7 5 3 6 0
Image 1Part, 18hargav Hdd/HTFSIRRECYC         rels         XML         Document         NA         1//1980 12:00:00.AM         NA         ST           Image 1Part, 18hargav Hdd/HTFSIRRECYC         door         MS Obcument         11/10/2018 4/37.31 PM         10/1/2018 2/30.34 AM         11/10/2018 4/37.31 PM         73,5           Image 1Part, 18hargav Hdd/HTFSIRRECYC         door         MS Obcument         11/10/2018 4/37.31 PM         10/1/2018 4/37.31 PM         73,5           Image 1Part, 18hargav Hdd/HTFSIRRECYC         door         MGresset Wex.         Document         11/10/2018 4/37.31 PM         10/1/2018 4/37.31 PM         24.97,7           Image 1Part, 18hargav Hdd/HTFSIRRECYC         xml         XML         Document         NA         11/1/1980 12:00:00 AM         NA         24.97,7           Image 1Part, 18hargav Hdd/HTFSIRRECYC         xml         XML         Document         NA         11/1/1980 12:00:00 AM         NA         24.97,7           Image 1Part, 18hargav Hdd/HTFSIRRECYC         xml         XML         Document         NA         11/1/1980 12:00:00 AM         NA         24.97,7           Image 1Part, 18hargav Hdd/HTFSIRRECYC         xml         XML         Document         NA         11/1/1980 12:00:00 AM         NA         24.97,7           Image 1Part, 18hargav Hdd/HTFSIRR	File Name fontTable.xml fontTable.xml fontTable.xml fontTable.xml fontTable.xml fontTable.xml fontTable.xml fontTable.xml		Full Path Hdd image 1/Part Hdd image 1/Part Hdd image 1/Part Hdd image 1/Part Hdd image 1/Part Hdd image 1/Part		Recycle Bi	Ext F xml Xi xml Xi xml Xi xml Xi xml Xi xml Xi xml Xi	ile Type ML ML ML ML ML ML ML	Document Document Document Document Document Document	Subject	N/A N/A N/A N/A N/A N/A	1/1/1980 12:00:00 AM 1/1/1980 12:00:00 AM 1/1/1980 12:00:00 AM 1/1/1980 12:00:00 AM 1/1/1980 12:00:00 AM 1/1/1980 12:00:00 AM 1/1/1980 12:00:00 AM	N/A N/A N/A N/A N/A N/A	3,823 2,797 3,356 2,983 3,386 1,450	7 5 3 6 0 5
End         food 22 door         Hdd image1Part_118hargav HddATFS\\$RECYC         door.         MS Office 12         Document         11/10/2018 4.37:31 PM         10/1/2018 2.08:34 AM         11/10/2018 4.37:31 PM         73.6           Image1/Part_118hargav HddATFS\\$RECYC         door.         Microsoft Wor         Document         11/10/2018 4.37:31 PM         10/1/2018 2.37:31 PM         10/1/2018 2.37:31 PM         10/1/2018 2.37:31 PM         10/1/2018 2.37:31 PM         2.497.7           Image1/Part_118hargav HddATFS\\$RECYC         door.         Microsoft Wor         Document         N/A         1/1/1980 12:00:00 AM         N/A         2.497.7           Image1/Part_118hargav HddATFS\\$RECYC         xml         XML         Document         N/A         1/1/1980 12:00:00 AM         N/A         2.497.4           Image1/Part_118hargav HddATFS\\$RECYC         xml         XML         Document         N/A         1/1/1980 12:00:00 AM         N/A         2.497.4           Image1/Part_118hargav HddATFS\\$RECYC         xml         XML         Document         N/A         1/1/1980 12:00:00 AM         N/A         2.497.4           Image1/Part_118hargav HddATFS\\$RECYC         xml         XML         Document         N/A         1/1/1980 12:00:00 AM         N/A         1.497.4           Image1/Part_118hargav HddATFS\\$RECYC	File Name fontTable.xml fontTable.xml fontTable.xml fontTable.xml fontTable.xml fontTable.xml fontTable.xml		Full Path Hdd image 1/Part Hdd image 1/Part Hdd image 1/Part Hdd image 1/Part Hdd image 1/Part Hdd image 1/Part Hdd image 1/Part		Recycle Bi	Ext F xml Xi xml Xi xml Xi xml Xi xml Xi xml Xi xml Xi xml Xi	ile Type ML ML ML ML ML ML ML ML	Document Document Document Document Document Document Document	Subject	N/A N/A N/A N/A N/A N/A N/A	1/1/1980 12:00:00 AM 1/1/1980 12:00:00 AM 1/1/1980 12:00:00 AM 1/1/1980 12:00:00 AM 1/1/1980 12:00:00 AM 1/1/1980 12:00:00 AM 1/1/1980 12:00:00 AM	N/A N/A N/A N/A N/A N/A N/A	3,823 2,797 3,356 2,983 3,386 1,450 2,516	7 5 3 6 0 5 9
Image 1/Part_18/mage 1/Part_	File Name font Table xmi		Full Path Hdd image 1/Part Hdd image 1/Part Hdd image 1/Part Hdd image 1/Part Hdd image 1/Part Hdd image 1/Part Hdd image 1/Part	L_1Bhargav Hdd.NTFSISRECYC. LIBnargav Hdd.NTFSISRECYC. LIBnargav Hdd.NTFSISRECYC. LIBnargav Hdd.NTFSISRECYC. LIBnargav Hdd.NTFSISRECYC. LIBnargav Hdd.NTFSISRECYC. LIBnargav Hdd.NTFSISRECYC. LIBnargav Hdd.NTFSISRECYC.	Recycle Bi	Ext         F           xml         X	ile Type ML ML ML ML ML ML ML ML ML	Document Document Document Document Document Document Document Document	Subject	N/A N/A N/A N/A N/A N/A N/A	1/1/1980 12:00:00 AM 1/1/1980 12:00:00 AM	N/A N/A N/A N/A N/A N/A N/A N/A	3,823 2,797 3,356 2,983 3,386 1,450 2,516 2,615	7 5 3 6 0 5 9 8
Image:         Description         NA         1/1/1980 120:000 AM         NA         2,2           Image:         Image:         Na         1/1/1980 120:000 AM         NA         2,2           Image:         Image:         Na         1/1/1980 120:000 AM         NA         2,6           Image:         Image:         Na         1/1/1980 120:000 AM         NA         1,1           Image:         Na         1/1/1980 120:000 AM         NA         1,1           Image:         Na         1/1/1980 120:000 AM         NA         1,1	File Name fontTable xmi fontTable xmi fontTable xmi fontTable xmi fontTable xmi fontTable xmi fontTable xmi fontTable xmi fontTable xmi fontTable xmi		Full Path Hdd image 1/Part Hdd image 1/Part		Recycle Bi	Ext F xml X xml X	ile Type ML ML ML ML ML ML ML ML ML ML ML	Document Document Document Document Document Document Document Document Document Document	Subject	N/A N/A N/A N/A N/A N/A N/A N/A N/A N/A	1/1/1980 12:00:00 AM 1/1/1980 12:00:00 AM	N/A N/A N/A N/A N/A N/A N/A N/A	3,822 2,791 3,356 2,983 3,386 1,456 2,518 2,618	7 5 3 6 0 5 9 8 1 9
Incoler1.xml         Hold image1Part_11Bhargav Hd-NTFSISRECYC         xml         Document         N/A         1/1/1980 12:00:00 AM         N/A         2,6           Information         Hold image1Part_11Bhargav Hd-NTFSISRECYC         xml         XML         Document         N/A         1/1/1980 12:00:00 AM         N/A         1,6	File Name fortTable.xmi fortTable.xmi fortTable.xmi fortTable.xmi fortTable.xmi fortTable.xmi fortTable.xmi fortTable.xmi fortTable.xmi fortTable.xmi fortTable.xmi fortTable.xmi fortTable.xmi		Full Path Hdd image 19an Hdd image 19an		Recycle Bi	Ext F xml X xml X	ile Type ML ML ML ML ML ML ML ML ML IS Office 12	Document Document Document Document Document Document Document Document Document Document	Subject	NA NA NA NA NA NA NA NA NA NA 1/10/2018 4:37:31 PM	1/1/1980 12:00:00 AM 1/1/1980 12:00:00 AM	N/A N/A N/A N/A N/A N/A N/A N/A 11/10/2018 4:37:31 PM	3,822 2,791 3,356 2,983 3,384 1,456 2,511 2,515	7 5 3 6 0 5 9 8 1 9 8
footer1.xml Hdd image1\Part_1\Bhargav Hdd-NTFS\\$RECYC xml XML Document N/A 1/1/1980 12:00:00 AM N/A 1,5	File Name font Table xmi font Table xmi		Full Path Hdd image19an Hdd image19an		Recycle Bi	Ext F xml X xml X xm	ile Type ML ML ML ML ML ML ML ML SML SOffice 12 Kicrosoft Wor	Document Document Document Document Document Document Document Document Document Document Document	Subject	NA NA NA NA NA NA NA NA NA NA 11/10/2018 4:37:31 PM 11/10/2018 4:37:31 PM	1/1/1980 12:00:00 AM 1/1/1980 12:00:00 AM	N/A N/A N/A N/A N/A N/A N/A N/A N/A N/A	3,822 2,797 3,356 2,983 1,456 2,516	7 5 3 6 0 5 9 8 1 9 8 1 9 8 6
	File Name fortTable xm fortTable xm		Full Path Hdd image 19an Hdd image 19an		Recycle Bi	Ext F xml X xml X xm	ile Type ML ML ML ML ML ML ML ML ML Soffice 12 IS Office 12 ML	Document Document Document Document Document Document Document Document Document Document Document Document	Subject	NA NA NA NA NA NA NA NA NA 11/10/2018 4:37:31 PM 11/10/2018 4:37:31 PM	1/1/1980 12:00:00 AM 1/1/1980 12:00:00 AM	N/A N/A N/A N/A N/A N/A N/A N/A N/A 11/10/2018 4:37:31 PM 11/10/2018 4:37:31 PM	3,822 2,793 3,356 2,983 1,456 2,516	7 5 3 6 5 9 8 1 9 8 6 5 8 6 5
i footer1.xml Hdd image1\Part_1\Bhargav Hdd-NTFS\\$RECYC xml XML Document N/A 1/1/1980 12:00:00 AM N/A 2,5	File Name font Table xmi font Table xmi		Full Path Hdd image1Part Hdd image1Part		Recycle Bi	Ext F xml X xml X xm	ile Type ML ML ML ML ML ML ML ML ML S Office 12 Kiorosoft Wor ML	Document Document Document Document Document Document Document Document Document Document Document Document Document	Subject	NA NA NA NA NA NA NA NA NA NA NA NA NA N	1/1/1980 12:00:00 AM 1/1/1980 12:00:00 AM	N/A N/A N/A N/A N/A N/A N/A N/A N/A 11/10/2018 4:37:31 PM 11/10/2018 4:37:31 PM N/A	3,822 2,797 3,356 2,983 1,456 2,516	7 5 3 6 0 5 9 8 1 9 8 1 9 8 6 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5
Tief footer1.xml Hdd image1\Part_1\Bhargay Hdd-NTES\SRECYC xml XML Document N/A 1/1/1980 12:00:00 AM N/A	File Name     fortTable.xmi     fortTable.x		Full Path Hdd image 19an Hdd image 19an		Recycle Bi	Ext F xml X xml X	ile Type ML ML ML ML ML ML ML ML ML IS Office 12	Document Document Document Document Document Document Document Document Document Document	Subject	NA NA NA NA NA NA NA NA NA NA 1/10/2018 4:37:31 PM	1/1/1980 12:00:00 AM 1/1/1980 12:00:00 AM	N/A N/A N/A N/A N/A N/A N/A N/A 11/10/2018 4:37:31 PM		3,82 2,79 3,35 2,98 3,38 1,45 2,51 2,61 2,61 2,61 2,63 1,87 94 73,95

Figure 87. Document Preview for HDD Image

When we click on one of the folders, we can recover it, and we can see the preview of the

folder in Hex code format as follows.

Overview Exp	plore	e Graphics	E-Mail	Searc	h Boo	kmark								
Evidence Items		File Status	File Categor	у	*	~	* 20 2	100 Mil 100	ଚା ଜୀ					
Evidence items: 2	2	KFF Alert Files: 0	Documents:	1449				Entropy Services	Lord House					
File Items	1	Bookmarked Items: 0	Spreadsheets:	27					00 01 00 00	00 0				
Total File Items: 5000	0 1	Bad Extension: 112	Databases:	0						00				
checked items: 0	0 8	Encrypted Files: 1	Graphics:	1664										
Unchecked Items: 5000	0 1	From E-mail: 0	Multimedia:	0	1									
Flagged Thumbnails: 0	0 1	Deleted Files: 2728	E-mail Messages:	0	1									
Other Thumbnails: 1664	4	From Recycle Bin: 0	Executables:	0										
Filtered In: 5000		Duplicate items: 790	Archives:	46	1									
		OLE Subitems: 541	Folders:	26										
Unfiltered Filtered		Flagged Ignore: 0	Slack/Free Space:	182	1									
All Items Actual Files		KFF lonorable: 0	Other Known Type:	195	1									
Hotodiring		Data Carved Files: 0	Unknown Type:	1411	Cursor posi	tion = I	0							
	_	Euli Path	~  T		lumns Recycle Bi.	×	DTZ File Type	Category	Subject	Cr Date	Mod Date	Acc Date	L-Size	
File Name	_	D V off Unfiltered		All Co	Recycle Bi.			Category	Subject			Acc Date 11/10/2018 4:03:44 PM	L-Size	48
File Name	_	D V OFF Unfiltered Full Path Hdd image1\Par	~  T	All Co	Recycle Bi.		File Type		Subject				L-Size	43 656
File Name	_	OFF Unfittered     Full Path     Hdd image1\Par     Hdd image1\Par	∽ ∏ _18hargav Hdd-NTFS	All Co	Recycle Bi.		File Type Folder	Folder	Subject	11/10/2018 4:03:44 PM	11/10/2018 4:03:44 PM 6/21/2018 9:57:47 PM	11/10/2018 4:03:44 PM	L-Size	
File Name Seleted SExtend SSSMVBBU	_	C C C C C C C C C C C C C C C C C C C	→ I Bhargav Hdd-NTFS _11Bhargav Hdd-NTFS	All Co	Recycle Bi.		File Type Folder Folder	Folder Folder	Subject	11/10/2018 4.03-44 PM 6/21/2018 9:57:47 PM	11/10/2018 4:03:44 PM 6/21/2018 9:57:47 PM 11/10/2018 4:37:55 PM	11/10/2018 4:03:44 PM 6/21/2018 9:57:47 PM	L-Size	
File Name  SDeleted  SExtend  SRSMVBBU  SRSMVBBU  SRECYCLE,BIN	_	Orr Unfiltered     Full Path     Hdd image1/Par     Hdd image1/Par     Hdd image1/Par     Hdd image1/Par     Hdd image1/Par	L1\Bhargav Hdd-NTFS 1\Bhargav Hdd-NTFS 1\Bhargav Hdd-NTFS	All Co	Recycle Bi.	. Ext	File Type Folder Folder Folder	Folder Folder Folder	Subject	11/10/2018 4:03:44 PM 6/21/2018 9:57:47 PM 11/10/2018 4:37:47 PM	11/10/2018 4:03:44 PM 6/21/2018 9:57:47 PM 11/10/2018 4:37:55 PM 11/10/2018 4:06:39 PM	11/10/2018 4:03:44 PM 6/21/2018 9:57:47 PM 11/10/2018 4:37:55 PM	L-Size	656 56
File Name SDeleted SExtend SREVCE BIN SREUCLE BIN SREUBSLL SRUDB11	_	Orr Unfittered     Full Path     Hdd imaget Near	LIBhargav HdsATFS LIBhargav HdsATFS LIBhargav HdsATFS LIBhargav HdsATFS LIBhargav HdsATFS LIBhargav HdsATFS LIBhargav HdsATFS	All Co	Recycle Bi.	. Ext	File Type Folder Folder Folder Folder Folder Folder	Folder Folder Folder Folder Folder Folder	Subject	11/10/2018 4:03:44 PM 6/21/2018 9:57:47 PM 11/10/2018 4:37:47 PM 11/10/2018 4:06:39 PM 11/10/2018 4:37:57 PM 11/10/2018 4:36:57 PM	11/10/2018 4:03:44 PM 6/21/2018 9:57:47 PM 11/10/2018 4:37:55 PM 11/10/2018 4:06:39 PM 11/10/2018 4:38:04 PM 11/10/2018 4:37:08 PM	11/10/2018 4-03-44 PM 8/21/2018 9:57:47 PM 11/10/2018 4:37:65 PM 11/10/2018 4:06:39 PM 11/10/2018 4:38:04 PM 11/10/2018 4:37:08 PM	L-Size	656 56 320 56 56
File Name Stoleted Sextend SRSMVBBU SREUCLE BIN SREUBELL SRJD0B11 SRJXV8E1	_	OFF Unfittered     Full Path     Hdd image1/Par	C Bhargav Hdd-NTFS 19Bargav Hdd-NTFS 19Bargav Hdd-NTFS 19Bargav Hdd-NTFS 19Bargav Hdd-NTFS 19Bargav Hdd-NTFS 19Bargav Hdd-NTFS	All Co SEctored SRECYC SRECYC SRECYC SRECYC SRECYC SRECYC	Recycle Bi.	. Ext	File Type Folder Folder Folder Folder Folder Folder Folder	Folder Folder Folder Folder Folder Folder	Subject	11/10/2018 4:03:44 PM 6/21/2018 9:57:47 PM 11/10/2018 4:37:47 PM 11/10/2018 4:37:57 PM 11/10/2018 4:37:57 PM 11/10/2018 4:38:57 PM 11/10/2018 4:37:32 PM	11/10/2018 4:03:44 PM 6/21/2018 9:57:47 PM 11/10/2018 4:37:55 PM 11/10/2018 4:06:39 PM 11/10/2018 4:38:04 PM 11/10/2018 4:37:08 PM 11/10/2018 4:37:47 PM	11/10/2018 4:03:44 PM 6/21/2018 9:57:47 PM 11/10/2018 4:37:65 PM 11/10/2018 4:38:04 PM 11/10/2018 4:38:04 PM 11/10/2018 4:37:08 PM 11/10/2018 4:37:47 PM	L-Size	656 56 320 56 56 56
File Name 50eleted SRSMVBU SRSMVBU SREUSELL SREUSELL SRUSUE11 SRUSUE11 SRUSUE11 SRUSUE11	_	Orr Unfittered     Full Path     Hdd image1/Par	UBhargav Hdd ATFS 18hargav Hdd-ATFS 18hargav Hdd-ATFS 18hargav Hdd-ATFS 18hargav Hdd-ATFS 18hargav Hdd-ATFS 18hargav Hdd-ATFS 18hargav Hdd-ATFS	All Co SSExtend SSExtend SSRECYC SSRECYC SSRECYC SSRECYC SSRECYC SSRECYC SSRECYC SSRECYC SSRECYC	Recycle Bi.	. Ext	File Type Folder Folder Folder Folder Folder Folder Folder Folder	Folder Folder Folder Folder Folder Folder Folder	Subject	11/10/2018 4 03:44 PM 6/21/2018 9:57:47 PM 11/10/2018 4:37:47 PM 11/10/2018 4:07:57 PM 11/10/2018 4:38:57 PM 11/10/2018 4:37:32 PM 11/10/2018 4:37:35 PM	11/10/2018 4:03:44 PM 8/21/2018 9:57:47 PM 11/10/2018 4:07:55 PM 11/10/2018 4:06:39 PM 11/10/2018 4:08:04 PM 11/10/2018 4:37:08 PM 11/10/2018 4:37:47 PM 11/10/2018 4:37:57 PM	11/10/2018 4:03:44 PM 6/21/2018 9:57:47 PM 11/10/2018 4:37:55 PM 11/10/2018 4:08:39 PM 11/10/2018 4:08:39 PM 11/10/2018 4:37:08 PM 11/10/2018 4:37:47 PM 11/10/2018 4:37:57 PM	L-Size	656 56 320 56 56 56 176
File Name SExtend SR8MVB8U SREUBSLL SREUBSLL SRJOB11 SRJOV8E1 SRJAV8E1 SRMLRE92 SRMMetadata	_	Worr Unfittered     Full Path     Hold (mage1)Pat	UBNargav Hdd-NTFS UBhargav Hdd-NTFS UBhargav Hdd-NTFS UBhargav Hdd-NTFS UBhargav Hdd-NTFS UBhargav Hdd-NTFS UBhargav Hdd-NTFS UBhargav Hdd-NTFS UBhargav Hdd-NTFS	All Co SSExtend SSExtend SSRECYC	Recycle Bi.	. Ext	File Type Folder Folder Folder Folder Folder Folder Folder Folder Folder	Folder Folder Folder Folder Folder Folder Folder Folder	Subject	11/10/2018 4 03:44 PM 6/21/2018 9:57:47 PM 11/10/2018 4:37:47 PM 11/10/2018 4:06:38 PM 11/10/2018 4:36:57 PM 11/10/2018 4:36:57 PM 11/10/2018 4:37:57 PM 6/21/2018 9:57:52 PM	11/10/2018 4:03:44 PM 6/21/2018 9:57:47 PM 11/10/2018 4:37:56 PM 11/10/2018 4:06:39 PM 11/10/2018 4:36:04 PM 11/10/2018 4:37:08 PM 11/10/2018 4:37:47 PM 11/10/2018 4:37:57 PM 6/21/2018 9:57:52 PM	11/10/2018 4:03:44 PM 6/21/2018 9:57:47 PM 11/10/2018 4:37:65 PM 11/10/2018 4:37:65 PM 11/10/2018 4:37:63 PM 11/10/2018 4:37:67 PM 11/10/2018 4:37:67 PM 6/21/2018 9:57:52 PM	L-Size	656 56 56 56 56 176 336
File Name File Name Statend SREVERU SREVESLL SRJ00811 SRJ00811 SRMetadata SRMetadata SRMetadata	_	Or Unffered     Unffered     Unffered     Unffered     Unffered     Hdd image1Par     Hdd     Hdd image1Par     Hd     Hdd     Hd	V Rishargav Hdd-NTFS (18hargav Hdd-NTFS (18hargav Hdd-NTFS (18hargav Hdd-NTFS (18hargav Hdd-NTFS (18hargav Hdd-NTFS (18hargav Hdd-NTFS (18hargav Hdd-NTFS (18hargav Hdd-NTFS (18hargav Hdd-NTFS	All Co SSExtend SSExtend SSECYC SSRECYC SSRECYC SSRECYC SSRECYC SSRECYC SSRECYC SSRECYC SSRECYC SSRECYC SSRECYC SSRECYC SSRECYC	Recycle Bi.	. Ext	File Type Folder Folder Folder Folder Folder Folder Folder Folder Folder	Folder Folder Folder Folder Folder Folder Folder Folder Folder	Subject	11/10/2018 4.03/44 PM 6/21/2018 9.57/47 PM 11/10/2018 4.37/47 PM 11/10/2018 4.37/57 PM 11/10/2018 4.36/57 PM 11/10/2018 4.36/57 PM 11/10/2018 4.37/35 PM 11/10/2018 4.37/35 PM 11/10/2018 4.37/35 PM	11/10/2018 4:03 44 PM 6/21/2018 9:57:47 PM 11/10/2018 4:37:56 PM 11/10/2018 4:36:39 PM 11/10/2018 4:36:38 04 PM 11/10/2018 4:37:38 PM 11/10/2018 4:37:57 PM 6/21/2018 9:57:52 PM 11/10/2018 4:37:32 PM	11/10/2018 4:03:44 PM 6/21/2018 9:57:47 PM 11/10/2018 4:37:65 PM 11/10/2018 4:08:39 PM 11/10/2018 4:38:04 PM 11/10/2018 4:37:08 PM 11/10/2018 4:37:47 PM 11/10/2018 4:37:57 PM 0/21/2018 9:57:52 PM 11/10/2018 4:37:32 PM	L-Size	656 56 320 56 56 176 336 176
File Name Steletad SEctend SREWSBU SREVCLE BIN SREUBAL SRUDB11 SRUD1	_	Vor Unflered     Full Path     Hold Invage119ar     Hold Invage119a	LIBhargav Hdd NTFE LIBhargav Hdd NTFE LIBhargav Hdd NTFE LIBhargav Hdd NTFS LIBhargav Hdd NTFS	All Co SSEction SSECYC SSRE	Recycle Bi.	. Ext	File Type Folder Folder Folder Folder Folder Folder Folder Folder Folder	Folder Folder Folder Folder Folder Folder Folder Folder Folder Folder	Subject	11/10/2018 4:03:44 PM 0/21/2018 9:57:47 PM 11/10/2018 4:03:47 PM 11/10/2018 4:06:38 PM 11/10/2018 4:06:38 PM 11/10/2018 4:06:57 PM 11/10/2018 4:37:56 PM 11/10/2018 4:37:56 PM 11/10/2018 4:37:59 PM 11/10/2018 4:37:39 PM	11/10/2018 4.03.44 PM 6/21/2018 5.67.47 PM 11/10/2018 4.57.56 PM 11/10/2018 4.37.56 PM 11/10/2018 4.37.68 PM 11/10/2018 4.37.69 PM 11/10/2018 4.37.47 PM 11/10/2018 4.37.57 PM 6/21/2018 5.67.52 PM 11/10/2018 4.37.32 PM 11/10/2018 4.37.32 PM	11/10/2018 4.03:44 PM 6/21/2018 9.57:47 PM 11/10/2018 4.37:85 PM 11/10/2018 4.37:85 PM 11/10/2018 4.37:85 PM 11/10/2018 4.37:85 PM 11/10/2018 4.37:47 PM 11/10/2018 4.37:47 PM 11/10/2018 4.37:32 PM 11/10/2018 4.37:32 PM	L-Size	656 56 320 56 56 176 336 176 56
File Name File Name Sterend SREWBU SREUBSLL SRUOB11 SRUX8E1 SRUX8E1 SRUX8E1 SRUX8E1 SRUX8E1 SRUX8E3 SRMEB2 SRMEB2 SRMEB2 SRMEB23 SRMEB23 SRMEB23 SRMEB23 SRMEB23 SRMEB23 SRMEB33 SRMEB33 SRME SRMEB33 SRME SRMEB33 SRME	_	Or Unftered     Full Path     Hod Image (Par     Hod Image (Par	() () () () () () () () () () () ()	All Co SSExtend SSExtend SSECYC SSRECYC	Recycle Bi.	. Ext	File Type Folder Folder Folder Folder Folder Folder Folder Folder Folder Folder	Folder Folder Folder Folder Folder Folder Folder Folder Folder Folder Folder	Subject	1110/2018 4 03 44 PM 621/2018 957 47 PM 111/0/2018 4 37 47 PM 111/0/2018 4 307 47 PM 111/0/2018 4 367 PM 111/0/2018 4 3657 PM 111/0/2018 4 37.56 PM 0/21/2018 957 62 PM 111/0/2018 4 37.56 PM 111/0/2018 4 37.57 647 09 111/0/2018 4 37.55 PM	11/10/2018 4.00:44 PM 0/21/2018 9.57:47 PM 11/10/2018 4.37:56 PM 11/10/2018 4.37:56 PM 11/10/2018 4.37:56 PM 11/10/2018 4.37:30 PM 11/10/2018 4.37:47 PM 11/10/2018 4.37:32 PM 11/10/2018 4.37:32 PM	11/10/2018 4:03:44 PM 6/21/2018 9:57:47 PM 11/10/2018 4:37:65 PM 11/10/2018 4:37:65 PM 11/10/2018 4:37:65 PM 11/10/2018 4:37:65 PM 11/10/2018 4:37:47 PM 11/10/2018 4:37:32 PM 11/10/2018 4:37:32 PM	L-Size	656 56 320 56 56 176 336 176 56
File Name File Name SREAVBU SREAVBU SRECVCLE BIN SRECVCLE BIN SREUBSLL SRLD0B11 SRLD0B11 SRLLEB2 SRMMetadata SRMMetadata SRMMPWG SRMMPS SRMMPS SRMS23G SRTK1UN	_	Vor Unflered     Full Path     Hold runge 10/ar     Hold runge 10/a	L I Bhagar Hdd NTFB L I Bhagar Hdd NTFB L I Bhagar Hdd NTFB L I Bhagar Hdd NTFB L I Bhagar Hdd NTFS L I Bhagar Hdd NTFS L I Bhagar Hdd NTFS L I Bhagar Hdd NTFF L I Bhagar Hdd NTFF	All Co SSEcted SSECYC SSRECYC SSRECYC SSRECYC SSRECYC SSRECYC SSRECYC SSRECYC SSRECYC SSRECYC SSRECYC SSRECYC SSRECYC	Recycle Bi.	. Ext	File Type Folder Folder Folder Folder Folder Folder Folder Folder Folder Folder Folder Folder	Folder Folder Folder Folder Folder Folder Folder Folder Folder Folder Folder Folder	Subject	11102018 4 03 4 94 04 94 04 94 04 94 04 94 04 94 04 94 04 94 04 04 04 04 04 04 04 04 04 04 04 04 04	11/10/2018 4.03 44 PM 0/21/2018 9.57.47 PM 11/10/2018 4.35 6 PM 11/10/2018 4.35 6 PM 11/10/2018 4.36 04 PM 11/10/2018 4.37.08 PM 11/10/2018 4.37.47 PM 11/10/2018 4.37.57 PM 11/10/2018 4.37.32 PM 11/10/2018 4.37.32 PM 11/10/2018 4.37.39 PM	11/10/2018 4.03.44 PM 6/21/2018 9.57.47 PM 11/10/2018 4.37.65 PM 11/10/2018 4.37.65 PM 11/10/2018 4.37.68 PM 11/10/2018 4.37.68 PM 11/10/2018 4.37.67 PM 6/21/2018 4.37.67 PM 11/10/2018 4.37.57 PM 11/10/2018 4.37.25 PM 11/10/2018 4.37.25 PM	L-Size	656 56 56 56 56 176 336 176 56 56 216
File Name File Name Sector	_	Vor Unftered     Full Path     Hod Image1Par	I I Brangew Hold NT FE I I Brangew Hold NT FE I Brangew Hold NT FE	All Co SSExtend SSEctor SSRECYC SSRECYC SSRECYC SSRECYC SSRECYC SSRECYC SSRECYC SSRECYC SSRECYC SSRECYC SSRECYC SSRECYC SSRECYC SSRECYC SSRECYC SSRECYC SSRECYC	Recycle Bi. A	. Ext	File Type Folder Folder Folder Folder Folder Folder Folder Folder Folder Folder Folder Folder	Folder Folder Folder Folder Folder Folder Folder Folder Folder Folder Folder	Subject	11102018-403-44 PM 6212018-57-47 PM 11102018-437-47 PM 11102018-437-57 PM 11102018-437-57 PM 11102018-437-57 PM 11102018-437-58 PM 11102018-437-58 PM 11102018-437-58 PM 11102018-437-58 PM 11102018-437-58 PM	11/10/2018 4.03 44 PM 0/21/2018 9.57.47 PM 11/10/2018 4.35 6 PM 11/10/2018 4.35 6 PM 11/10/2018 4.36 04 PM 11/10/2018 4.37.08 PM 11/10/2018 4.37.47 PM 11/10/2018 4.37.57 PM 11/10/2018 4.37.32 PM 11/10/2018 4.37.32 PM 11/10/2018 4.37.39 PM	11/10/2018 4:03:44 PM 6/21/2018 9:57:47 PM 11/10/2018 4:37:65 PM 11/10/2018 4:37:65 PM 11/10/2018 4:37:65 PM 11/10/2018 4:37:65 PM 11/10/2018 4:37:47 PM 11/10/2018 4:37:32 PM 11/10/2018 4:37:32 PM	L-Size	656 56 320 56 56 176 336 176 56
File Name     Solidiid     Skend     Skend     SkeubalL     SkubalL     S	_	Vor Unflered     Full Path     Hold runge 10ar     Hold runge	L I Bhagar Hdd NTFB L I Bhagar Hdd NTFB L I Bhagar Hdd NTFB L I Bhagar Hdd NTFB L I Bhagar Hdd NTFS L I Bhagar Hdd NTFS L I Bhagar Hdd NTFS L I Bhagar Hdd NTFF L I Bhagar Hdd NTFF	All Co All Co	Recycle Bi.           X           Z <td>. Ext</td> <td>File Type Folder Folder Folder Folder Folder Folder Folder Folder Folder Folder Folder Folder</td> <td>Folder Folder Folder Folder Folder Folder Folder Folder Folder Folder Folder Folder Folder</td> <td>Subject</td> <td>11102018 4 03 4 94 PM 6212018 957 47 PM 11102018 4 37 47 PM 11102018 4 39 47 PM 11102018 4 38 57 PM 11102018 4 38 57 PM 11102018 4 37 58 PM 10102018 4 37 58 PM 11102018 4 37 59 PM</td> <td>11/10/2018 4.00:44 PM 0/21/2018 9.57:47 PM 11/10/2018 4.37:56 PM 11/10/2018 4.37:56 PM 11/10/2018 4.37:56 PM 11/10/2018 4.37:38 PM 11/10/2018 4.37:37 PM 0/21/2018 4.37:37 PM 11/10/2018 4.37:37 PM 11/10/2018 4.37:37 PM 11/10/2018 4.37:36 PM 11/10/2018 4.37:36 PM</td> <td>11/10/2018 4:03:44 PM 6/21/2018 9:57:47 PM 11/10/2018 4:37:65 PM 11/10/2018 4:37:65 PM 11/10/2018 4:37:65 PM 11/10/2018 4:37:65 PM 11/10/2018 4:37:65 PM 11/10/2018 4:37:15 PM 11/10/2018 4:37:15 PM 11/10/2018 4:37:05 PM 11/10/2018 4:37:05 PM 11/10/2018 4:37:05 PM</td> <td>L-Size</td> <td>656 56 320 56 56 56 176 336 176 56 216 56</td>	. Ext	File Type Folder Folder Folder Folder Folder Folder Folder Folder Folder Folder Folder Folder	Folder Folder Folder Folder Folder Folder Folder Folder Folder Folder Folder Folder Folder	Subject	11102018 4 03 4 94 PM 6212018 957 47 PM 11102018 4 37 47 PM 11102018 4 39 47 PM 11102018 4 38 57 PM 11102018 4 38 57 PM 11102018 4 37 58 PM 10102018 4 37 58 PM 11102018 4 37 59 PM	11/10/2018 4.00:44 PM 0/21/2018 9.57:47 PM 11/10/2018 4.37:56 PM 11/10/2018 4.37:56 PM 11/10/2018 4.37:56 PM 11/10/2018 4.37:38 PM 11/10/2018 4.37:37 PM 0/21/2018 4.37:37 PM 11/10/2018 4.37:37 PM 11/10/2018 4.37:37 PM 11/10/2018 4.37:36 PM 11/10/2018 4.37:36 PM	11/10/2018 4:03:44 PM 6/21/2018 9:57:47 PM 11/10/2018 4:37:65 PM 11/10/2018 4:37:65 PM 11/10/2018 4:37:65 PM 11/10/2018 4:37:65 PM 11/10/2018 4:37:65 PM 11/10/2018 4:37:15 PM 11/10/2018 4:37:15 PM 11/10/2018 4:37:05 PM 11/10/2018 4:37:05 PM 11/10/2018 4:37:05 PM	L-Size	656 56 320 56 56 56 176 336 176 56 216 56

Figure 88. Folders Hex Code for HDD Image

74

## Summary

In this chapter, we have loaded data into HDD and SSD and created images using FTK Imager. Next step is to load those images and analyze them as per digital forensic techniques. Analyze the results and conclusions are given in the next chapter.

### **Chapter V: Results, Conclusion, and Recommendations**

### Introduction

In this chapter, we will be comparing results and deriving the conclusion about the findings.

#### Results

### Comparison of file hits in HDD vs. SSD.

#### Table 2

### Comparison of Hits in HDD and SSD

		DD /2018		SSD 4/2018
Contents	No of Hits	No of files	No of Hits	No of files
Animal	1676	39	249	42
Travel	1147	11	763	95
Plant	2053	55	426	33
Sunshine	808	4	37	14
Doc files	3716	182	584	1498
PDF files	2688	102	161	1726
Excel files	5	5	399	366

## Comparison of file hits in various images of Solid-State Drives.

## Table 3

# Comparison of File Hits in Various Images of Solid-State Drives

	7/4/2018 SS	•	7/14/2018 SSI	- Day 10 - D 2	7/24/2018 SSI	•		8 - Day 30- SD 4
Contents	No. of Hits	No. of Files	No. of Hits	No. of Files	No. of Hits	No. of Files	No. of Hits	No. of files
Animals	249	42	23	5	12	6	0	0
Travel	763	95	2	1	1	1	0	0
Plant	426	33	5	4	0	0	0	0
Sunshine	37	14	9	6	6	4	0	0
Doc files	584	1498	1420	1206	1245	1073	0	0
PDF files	161	1726	235	228	1971	1310	0	0
Excel files	399	366	4519	1441	260	245	0	0

### Pictorial representation.





Figure 89. Comparison of All Images vs. Recovered Data

#### Conclusion

Based on our findings we clearly understand that the performance of SSD's is far beyond expectations to that of HDD's. When we use FTK to analyze our results, we can see that we can recover deleted files from the HDD. However, in the case of SSD, we have created four images, and we can see that the file count has been decreasing over time. It becomes a massive problem to the investigators as they cannot recover the deleted data.

When the forensic investigators collect the SSD as evidence, it is not possible for them to start the investigation right away. It has many processes before they can start looking at the evidence. By this time the data in the SSD will have been vanished and would not have any critical pieces of evidence to prove the case. There need to be some advanced tools and techniques to retrieve data from these devices.

#### **Future Work**

As a future work, it is recommended to come up with a change in the design of the solidstate drive with a switch which can disable the pre-clearing function of the drive. With the use of this switch, it becomes easier to stop automatic erasing of the data from the drive and preserve the data for the forensic experts. The switch can be implemented in the form of a magnetic switch integrated into the solid-state drive package which can be activated via a magnet that is placed outside this package case. When the switch is activated, this will give a signal to the processor or the controller to disable the pre-clearing function of the solid-state drive.

#### References

- Bednar, P., & Katos, V. (2011). SSD: New challenges for digital forensics. In A. D'Stri, D.
  Te'enie, & M. De Marco (Eds.), *Information systems: A crossroads for organization, management, accounting, and engineering*. Retrieved from https://portal.research.lu.se/ws/files/5456453/4318024.pdf
- Bell, G. B. (2010). Solid state drives: The beginning of the end for current practice in digital forensic recovery. *The Journal of Digital Forensics, Security and Law*, 5(3), 1-20.
- Brendan, H. (2017). *The battle between SSD and HDD is over, and the winner is clear*. Retrieved from https://www.yahoo.com/tech/battle-between-ssd-hdd-over-141508916
- Bux, W., & Iliadis, I. (2010). Performance of greedy garbage collection in flash-based solidstate drives. *Performance Evaluation*, 67(11), 1172-1186.
- C/net. (n.d.). *Digital storage basics, Part 4: SSD explained*. Retrieved from Cnet: https://www.cnet.com/how-to/digital-storage-basics-part-4-ssd-explained/
- Chen, F. K. (2011). Making the best use of solid state drives in high-performance storage systems. In Proceedings of the International Conference on supercomputing, (ACM), pp. 22-32.
- Geier, F. (2015). The differences between SSD and HDD technology regarding forensic investigations. Sweden: Linnaeus University. Retrieved from http://www.gti.bh/Library/assets/fulltext01-gshhsy652.pdf
- INFOSEC. (n.d.). 7 best computer forensics tools. Retrieved from http://resources.infosecinstitute.com/7-best-computer-forensics-tools/#gref

- King, C., & Vidas, T. (2011). Empirical analysis of solid state disk data retention when used with contemporary operating systems. *Digital Investigation*, 8(Supplement), S111-S117.
- Phelps, J. (2012). How to partition and format your hard drive in windows. Retrieved from *PC World*, https://www.pcworld.com/article/248980/how-to-partition-and-format-your-harddrive-in-windows.html
- Ries, D. G., & Hill, C. (2017). Digical forensics in the courts. Retrieved from https://www.duq.edu/assets/Documents/forensics/\_pdf/Forensic%20Fridays/March%202 4%202017/Ries%20Digital%20Forensics%20Handout%203-24-17.pdf

Technopedia. (n.d.). In Wikipedia. Retrieved from https://www.techopedia.com/

- Thierolf, T., & Uriarte, J. (2010). Solid state drive architecture: A comparison and evaluation of data storage mediums. Retrieved from http://meseec.ce.rit.edu/551-projects/fall2010/1-4.pdf
- Wei, M. G., Grupp, L. M., Spada, F. E., & Swanson, S. (2011). Reliably erasing data from flashbased solid state drives. In *Proceedings of 9<sup>th</sup> USENIX Conference on File and Storage Technologies (FAST '11)*, San Jose, CA.
- Woodford, C. (2018). *Hard drives*. Retrieved from https://www.explainthatstuff.com/ harddrive.html
- Zhao, K. Z., Zhao, W., Sun, H., Zhang, T., Zhang, X., & Zheng, N. (2013). LDPC-in-SSD:
  Makng advanced error correction codes work effectively in solid state drives. In *Proceedings of 11th USENIX Conference on File and Storage Technologies* (FAST'13),
  San Jose, CA.