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

Culminating Projects in Information Assurance

Department of Information Systems

5-2018

# Different Forensic Tools on a Single SSD and HDD, Their Differences and Drawbacks

Yashwanth Reddy Kambalapalli *St. Cloud State University*, ykambalapalli@stcloudstate.edu

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

**Recommended** Citation

Kambalapalli, Yashwanth Reddy, "Different Forensic Tools on a Single SSD and HDD, Their Differences and Drawbacks" (2018). *Culminating Projects in Information Assurance*. 59. https://repository.stcloudstate.edu/msia\_etds/59

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.

### Different Forensic Tools on a Single SSD and HDD, Their Differences and Drawbacks

by

Yashwanth Reddy Kambalapalli

A Starred Paper

Submitted to the Graduate Faculty of

St. Cloud State University

in Partial Fulfillment of the Requirements

for the Degree

Master of Science

in Information Assurance

May, 2018

Starred Paper Committee: Mark Schmidt, Chairperson Paul Safonov Balasubramanian Kasi

#### Abstract

With the increase in technology comes great innovations. One such transformation is changing from Hard Disks to Solid State Drives. Solid State Drives generally known as SSD's is a nonvolatile memory which became a key storage system nowadays. SSD's are nothing but a storage device like Hard Disks but many times faster with a very much lower power consumption. They are smaller in size and more efficient, the mechanism by which SSDs store and modify data is intrinsically different from hard disk drives. Each innovation has its advantages as well as drawbacks. When it comes to digital forensics working on SSD's is relatively new. It has been a challenge for the cyber-crime investigators ever since the evolution of SSD's, it was easy in hard disks to retrieve deleted data but when it comes to SSD's, they can automatically retrieve or alter data whenever they are connected to power even without an interface which results in major evidence loss or contamination. There are different types of SSD's which do not function similarly is also a challenge to a cybercrime investigator. The main purpose of this paper is to describe the evolution of SSD's and creating image files of a single SSD and Hard Disk using different forensic tools and comparing results. We create an evidence file and pass it to SSD and HDD with multiple permutations and combinations, then we format the disks and create an image file of both the disks to analyze using a forensic tool. We will also analyze how many evidence files are being deleted completely from both the devices by comparing them with the original number files we passed and the original hits we obtained while performing the analysis on single evidence folder.

# **Table of Contents**

	Page
List of Tables	5
List of Figures	6
Chapter	
I. Introduction	11
Introduction	11
Problem Statement	14
Objective of the Study	15
II. Background and Literature Review	16

I.	Introduction	11
	Introduction	11
	Problem Statement	14
	Objective of the Study	15
II.	Background and Literature Review	16
	Digital Forensic	16
	Digital Forensic Process	19
	Digital Forensic Tools	20
	Evolution of SSD	25
	Advantages of SSD	30
III.	Methodology	33
	Hard Disk Drives	33
	Solid State Drives	35
	Hardware and Software Requirements	38
	Summary	39
IV.	Data Presentation and Analysis	40
	Introduction	40

Chapter
---------

Data Presentation	40
Data Analysis	54
Summary	60
V. Introduction, Results and Conclusion	61
Introduction	61
Results	61
Conclusion	84
References	85

Page

## List of Tables

Table		Page
1.	Results Obtained from Images of HDD in FTK	74
2.	Results Obtained from Images of SSD in FTK	76
3.	Comparing the Results Obtained in FTK	77
4.	Results Obtained from Images of HDD in Autopsy	82
5.	Results Obtained from Images of SSD in Autopsy	82
6.	Comparing the Results Obtained in Autopsy	82

# List of Figures

Figure		Page
1.	Solid state drives	12
2.	Digital forensic process	17
3.	Digital forensics process step-by-step	20
4.	Digital forensic framework	22
5.	X-Ways UI	24
6.	Encase UI	25
7.	SSD internal structure	26
8.	V-NAND SSD	28
9.	Evolution of SSD	29
10.	Usage of SSD and HHD comparison	30
11.	Hard disk drive image	33
12.	Hard disk internal structure	34
13.	Solid state drives	36
14.	Evidence folders	41
15.	Evidence car folder	41
16.	Evidence medicine folder	41
17.	Evidence farm house folder	42
18.	Evidence phone folder	42
19.	Evidence laptop folder	42
20.	Combined file size of the evidence, evidence thrashes, and junk file	43

Figure		Page
21.	Installation of HD shredder	44
22.	Running HD shredder	44
23.	Detecting both the drive on two different laptops	45
24.	Drive wiping process at random intervals in HDD and SSD	45
25.	Successful completion of disk wiping using HD shredder	46
26.	Passing evidence	46
27.	Passing Evidence 1, Evidence 2	47
28.	Passing Evidence 1, Evidence 3	47
29.	Passing Evidence 1, Evidence 4	47
30.	Passing Evidence 2, Evidence 3	48
31.	Passing Evidence 2, Evidence 4	48
32.	Passing Evidence 2, Evidence 4	48
33.	Selecting the source evidence	49
34.	Creating the image of a folder	49
35.	Selecting the source path	50
36.	Assigning name for unique identification	50
37.	Assigning image destination	51
38.	Selecting the fragmentation size	51
39.	Processing of image creation	52
40.	Verifying results of the image created	52
41.	Image summary for image	53

Page
1 490

Figure		Page
42.	Image of evidence folder	53
43.	Filling personal details of investigator	54
44.	Adding image file to FTK toolkit	55
45.	Adding image file to analyze	55
46.	Evidence summary and add evidence	56
47.	Extracting the files from image	56
48.	Home page of FTK toolkit	57
49.	Searching by the file names	57
50.	Home page of forensic imager	58
51.	Selecting image to convert	58
52.	Source of destination file forensic imager	59
53.	Image converted and summary	59
54.	HDD connected to Laptop 1	61
55.	Home screen of FTK	62
56.	Selecting option from type of device	62
57.	Selecting HDD drive from image creation	63
58.	Create image evidence item information	63
59.	Selecting the destination for image of HDD	54
60.	Create image destination path	54
61.	Selecting the type of image format	55
62.	Unique identification for the image file	55

63.	Selecting the fragmentation size for image of HDD	66
64.	Verifying and starting the process of image creation	66
65.	Image creation of HDD at different intervals	67
66.	Image created of HDD	67
67.	SSD connected to second laptop	68
68.	Selecting the logical drive for DDS image creation	68
69.	Selecting SSD drive for image creation	68
70.	Selecting the destination for image of SSD	69
71.	Selecting the type of SSD image	69
72.	Selecting the fragmentation size for image of SSD	69
73.	Verifying and starting the process of image creation of SSD	70
74.	Image creation of SSD at different intervals	70
75.	Images created of SSD	71
76.	Processing image 1 of HDD	71
77.	Files identified by searching keywords in image 1 of HDD	72
78.	Results identified in image 1 of HDD	72
79.	Processing image 2 of HDD	72
80.	Results identified in image 2 of HDD	73
81.	Files identified by searching keywords in image 2 of HDD	73
82.	Adding evidence to analyze results of SSD	84
83.	Processing Image 1 of SSD	84

# Figure

Figure		Page
84.	Processing image 2 of SSD	75
85.	Processing image 3 of SSD	75
86.	Processing image 4 of SSD	76
87.	Processing image 5 of SSD	76
88.	Difference in results identified by number of files in FTK	77
89.	Difference in results identified by number of Hit in FTK	78
90.	New case information	78
91.	Set case number and examiner	79
92.	Creating a case database	79
93.	Creating new text index	80
94.	Selecting type of data source	80
95.	Browsing image file	81
96.	Configure ingest modules	81
97.	Difference in results identified by number of files in autopsy	83
98.	Difference in results identified by number of Hit in autopsy	83

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

#### Introduction

Solid State Drives generally known as SSD's are non-volatile memory which became a key storage system nowadays, SSD can also be called as Solid State Disk, use of SSD is simple enough and for many purposes it can be used as if it was a normal hard disc but many times faster and with a very much lower power consumption, they are smaller in size and more efficient, it stores data in a persistent manner and Solid State Drives doesn't have any disks in a traditional manner that are spinning which stores data with two heads read and write. SSD in place of this mechanical device consists of integrated circuits and semiconductors which are used as memory devices. SSD does not have any magnetic tapes or optical storage media like in Hard Disks (Rouse, 2016).

Input and output operational performance is relatively high when compared to Hard drives which resulted in rapid growth in the use and evolution of SSD. HDDs have much greater random access and read access latency compared to SSDs, this lower random access and read access makes the SSDs reliable and efficient for both heavy read and random workloads. The ability of SSD to read data directly from the cell location is the reason for the lower latency (Rouse, 2016).

Flash memory based Solid State Drives (SSD), an emerging storage technology, plays a critical role in revolutionizing the storage system design. Such a fundamental difference makes SSD capable of providing one order of magnitude higher performance than rotating media and makes it an ideal storage medium for building high-performance storage systems. Due to the relatively low capacity and higher price which can accommodate more data compared to a

typical HDD will (Chen, Koufaty, & Zhang, 2016). As our computer is equipped with chips and motherboard comes with some of the chips which are called as system memory which is also called as RAM, is used to store and process data when a system is working, this is known as Volatile memory, the word volatile is used because the memory that is stored and accessed is removed as soon as the system is turned off or shut down. The microchips that are used in the Solid State Drives are called as the Non-Volatile memory because data will be stored in the device even after the system is turned off (Harris, 2015). Chips of SSD are not located on the motherboard. These chips are stored in another part of the computer, we can remove the hard drive of your laptop and replace it with a solid-state drive, without affecting any other essential components (Harris, 2015).





There are two types of Solid State Drives based on the mechanism they are built, NOR and NAND. Both NOR and NAND contains transistors and the cells where memory is stored. The wiring between these cells differs from each other as they follow different mechanism. In NOR the cells are wired in a parallel mechanism as it contains more complex structure and bigger structure and has more wires to connect and NAND these cells are arranged in a series mechanism where the complexity is much less as it contains fewer wires and they are packed on a chip with great density (Harris, 2015).

Because of this complex arrangement the NAND devices are cheaper and much used as the read and write operations are performed with a great speed. These features make NAND devices much more predominant memory storage device in Solid State Drives. NOR devices are mostly used when the data has read-only permission where the read access is much faster compared to NAND and the data is stored in a low density. Based on the above features of a solid-state drive, it can be defined "NAND flash to provide non-volatile, rewritable memory." (Harris, 2015).

Digital forensics plays an import role in the investigation due to the increase in the use of computers. Usage of computers has been predominantly increased in everyday human life which also involves criminal activities in some form that makes digital forensics role important in the investigation. Every crime nowadays will leave a trace of evidence in digital form, for example, usage of mobile phones, laptops, internet etc. finding these evidences and dig down to conclude will involve few methods and procedures. Digital forensic involves four steps in every investigation (Garfinkel, 2013).

Different forensic tools working on a single SSD, comparing the results of forensic tools on an SSD and the challenges faced by the forensic investigators are discussed in this paper.

#### **Problem Statement**

Due to increase of crime in both criminal, digital and civic activities, it has been a bottleneck situation for the investigators. As every crime nowadays involve electronic devices in some form whether it can be a direct hacking or a crime where an electronic device has been recovered as an evidence, investigators are more focusing on forensic science to know the motive of the crime or mindset of an individual.

There are many cases which can be solved using digital forensics. Technology is updating every day and use of latest devices has been increasing rapidly which makes investigators job a little more difficult compared to past. As people are updated with the technology and latest devices even investigators must focus more on the latest devices how they work and internal functioning of the device.

Digital forensic investigators more focus on traditional ways such as working on the hard drives as most of the devices are equipped with them from the past few decades and certain ways to drill down and find the evidence traditionally. However, these mechanisms cannot be applied on SSDs as they follow different storage mechanism and accessing data.

The difficulties faced by the forensic team to investigate on SSDs are discussed in this paper, this paper will also discuss what are the difficulties faced by the investigators when working on SSD compared to hard drives, different forensic tools work differently based on the budget allocated and the type of tool used to investigate. Each forensic tool will perform the different operation based on the capacity.

# **Objective of the Study**

- 1. The main objective of the study is to find out what are the challenges faced by the forensic investigators for finding evidence in SSD's.
- 2. This study will also compare the results obtained from different forensic tools on a single SSD and HDD.

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

#### **Digital Forensic**

Digital forensics plays an import role in the investigation due to the increase in the use of computers. Usage of computers has been predominantly increased in everyday human life which also involves criminal activities in some form that makes digital forensics role important in the investigation. Every crime nowadays will leave a trace of evidence in digital form, for example, usage of mobile phones, laptops, internet etc. finding these evidences and dig down to conclude will involve few methods and procedures. The process of uncovering and finding the evidence stored in any kind of an electronic device is called as "Digital Forensics" (Garfinkel, 2013).

Digital forensic investigators face a challenging role in computers when it comes to data analysis and cybersecurity. Forensic science is very much different from digital forensics as the data in a system can be changed and there is a vast data to analyze as well as the breakdown of everything to find out evidence, the process of digital forensics is never easy and timeconsuming as it may take months to years based on the complexity. Digital forensics nowadays is playing a major role in the investigation, it is acting as a breakpoint where it leads to a conclusion or gives a major hint in any crime. Digital forensics is also playing a major role in border security in scanning the emails and personal electronic equipment to ensure security. A digital forensic investigator must understand data and make sense of data found in a device and it is a very difficult task.



#### Figure 2: Digital forensic process (Azemovic, 2010).

Digital forensics in a real world serves two purposes each differ but they are in common with the investigation. First, an electronic device contains an evidence of a crime that occurred in a real world, due to the complexity of data in computers it made hard for the forensics team to analyze data on computer storage device than that of a paper record. For example, Bernard Madoff who made a financial scam in 1980, kept track of all the records of his victims on an IBM computer. Investigators have found the data using some tools back in those days to analyze data on his system and provide evidence of his crime. Suspects in a murder case generally have an electronic device involved in one way or the other. Digital forensics has now become part of every criminal as well as civil crime investigations (Garfinkel, 2013).

The second class is that a crime which involves the complete use of a system where a person is involved in a crime using a computer or an electronic device, hacking into other system and stealing data is one example of this class, here digital forensics plays a major part in the investigation. Dealing with these crimes it is very hard for a forensic investigator without a tool to analyze user data found in a hacker's laptop. Digital forensics is typically hard to analyze on the windows system as all the log files are hard to analyze manually and the junk data or the unwanted data that is present on the computer makes an investigation much more difficult than

usual, this also helps investigator to recover the data that has been deleted in the past using these log files and the data recovery process. Search history can be found in the system which can lead to a breakthrough in the investigation to draw a conclusion. These files will give an idea of a state of mind of a criminal. When it comes to the evidence like letters, photos can be submitted to the lawyers and judges. For example, a digital camera shows that it has around n images, but expert examination can retrieve that it has (n + y) images where y are the images deleted or erased, a person who delete or erase an image think it has been deleting permanently but data is never erased completely, it is stored in slack space (Garfinkel, 2013).

As the digital forensics consider the past and recover the data that has been deleted, this can also be applied to network security to check the intrusions and hacking. This is done not only to find a criminal but to find the loopholes in the network and to cover the holes in the system. Digital forensics also involves in finding data from the damaged disks or reformed. For example, In May 2006 a laptop and external hard drive that contains data of millions of veterans and military personnel have been stolen from military affairs official. After that laptop and hard disk were recovered the investigators used tools to check the data present in it and concluded that the files present on the hard drive were not affected or in fact, they are not viewed at all (Garfinkel, 2013). Digital forensics rely on the tools and forensic kits for investigation. It follows a step-by-step procedure in identifying the evidence, each evidence is analyzed in a different form such as a device found in a murder crime is investigated in a different way when it comes to a device found in a burglary. Investigation procedure is same, but the approach differs from each other. Before a device is analyzed it must be recovered properly and set to a state that the data present in the device is not fabricated. When the data are not properly handled

when the data present in the device can be altered leading to a false conclusion. Modern day devices had memory card and drives which store data in sectors generally 512 to 4096 bytes. A sector is the smallest part of a memory device where the actual data is stored. Each sector in the device has an id or a unique identifier called as "Sector Identification Number" or "Logical Block Address". Metadata is stored in some sectors where the data about the data is stored. RAM is also identified during the forensic process where an image is created to work on it as data in RAM will be erased as soon as the system is turned off (Garfinkel, 2013).

#### **Digital Forensic Process**

Digital Forensic process generally involves four steps they are preservation, overview, analysis, and reporting.

**Preservation**. This step focuses more on documentation and prevention of the evidence altering, in this step the device that is recovered by the forensic team will be preserved so that the data is not fabricated or changed. An image file is created for the device and the hash value is generated to validate the evidence in future if it is changed or not. This is the crucial step in the digital forensic process. (Dennon, 2016)

**Overview/examination**. The second step in the digital forensic process is called as overview or examination, here the hash value that is created for the device is checked and the image file that is generated is checked if it is successfully generated. The digital image format is generated (for example, image.EO1 file) (Dennon, 2016).

Analysis. The Third step in digital forensic is called an analysis where the actual work on the devices takes place which includes the process of user activity analysis which means log file analysis and browser history, deleted file recovery, retrieving the deleted files from the disk and keyword searching. It takes more time and effort in the entire forensic process (Dennon, 2016).

**Reporting**. Reporting is the final step in the digital forensic process where the evidence that is collected after the analysis is subjected to the conclusion and a human interactive written format is generated to present it in a courtroom or for the officials (Dennon, 2016).



Figure 3: Digital forensics process step-by-step (Janorkar, 2015).

#### **Digital Forensic Tools**

Digital Forensics require tools and kits to work on the device, there are many tools which are paid as well as open source, based on the purpose and the budget the tool used varies from case to case or the department it is investigating. The computer forensic tools can be classified as follows:

- 1. Disk and data capture tools
- 2. File viewers
- 3. File analysis tools
- 4. Registry analysis tools

- 5. Internet analysis tools
- 6. Email analysis tools
- 7. Mobile devices analysis tools
- 8. Mac OS analysis tools
- 9. Network forensics tools
- 10. Database forensics tools

Various forensic tools are available in the market:

**Forensic tool kit**. Forensic Tool Kit also known as FTK is a computer forensics software developed by Access Data. It is used in the digital investigation of hard drives, it creates an image file using FTK Imager, investigators work on the image file to find the evidence and such as deleted emails, deleted images, files. FTK imager creates an image file where it saves the hard disk data to be referenced in future if any changes are made to the hard drive data. A hash value is also generated to check for the future reference (wiki, 2017).

FTK allows handling huge data as it follows database-driven architecture. FTK has the flexibility of built-in visualization tools and detects images which help in reporting the relevant evidence that is found in an investigation. FTK has a feature of correlating data from different sources which include SSDs or hard drives, mobile phones, and other internet related devices. It reduces the investigation time which makes it a most preferred forensic tool (AccessData, 2017). FTK has features like Rainbow hashing tables and PORT.

**Digital Forensic Framework**. Digital Forensic Framework is a platform that is developed for the forensics, it has a user interface and is an open source tool available in the market, it is so user-friendly that anyone can use it without any trouble.



Figure 4: Digital forensic framework (Tools, 2014).

It can be used by both the digital forensic professionals as well as the beginners without any trouble. It can be used for multiple purposes such as digital chain of custody for accessing both the local and remote devices, for the forensics of both Windows operating system and Linux operating system. It also recovers the deleted data or the hidden files from a hard drive (Shankdhar, 2017). It has software write blocker which prevents from data manipulation or modification and has a cryptographic hash value calculator which is used for the future reference if the data is modified or not. It has the flexibility to read RAW, AFF and Encase EWF formats, it is also VMware compatible, it processes local files, binary files, and penetration testing (S.A.S., 2017).

**Open Computer Forensic Architecture**. Open Computer Forensics Architecture (OCFA) is a digital forensic tool, it is a popular open source framework available in the market. This was developed on the Linux platform and uses PostgreSQL for data storage. It was built by the police agency for digital forensics process of automation (Shankdhar, 2017).

**CAINE**. CAINE is also called as Computer Aided Investigation Environment is developed on the Linux platform which is created mainly for digital forensics. It is an open source tool available in the market (Shankdhar, 2017).

**X-Ways Forensic tool**. X-Ways Forensics is a digital forensic tool used for the advanced options. It is based on the Windows platform where it works on almost all the windows operating system. It claims to not be very resource hungry and to work efficiently. some of the features are listed below (X-Ways, 2017a).

Disk imaging and cloning, Ability to read file system structures inside various image files. It supports most of the file systems including FAT12, FAT16, FAT32, exFAT, TFAT, NTFS, Ext2, Ext3, Ext4, Next3®, CDFS/ISO9660/Joliet, UDF.

Automatic detection of deleted or lost hard disk partition, Various data recovery techniques and powerful file carving, Bulk hash calculation, Viewing and editing binary data structures using templates, Easy detection of and access NTFS ADS, Well maintained file header, Automated activity logging, Data authenticity, Complete case management, Memory and RAM analysis, Gallery view for pictures, Internal viewer for Windows registry file, Automated registry report, Extracts metadata from various file types, Ability to extract emails from various available email clients" (Shankdhar, 2017).

🔜 X-Ways Forensics - [NTFS Image.e01]												_	
🥪 File Edit Search Position View Tools	Specialist Options Window Help											_	8 ×
▶ 🗃 🖶 🗃 🚰 🖢 🗇 ங  🐘 🛔 🎄 🤽 ※ 📋 → 🕩 🗢 💠 │ 🥔 🖬 🧇 🚥 🔎 │ 🆽 体 🕨 👘 💮 🖽 │													
Case Data	[NTFS Image.e01]												
File Edit	▼\Pictures and subdirectories										74+1	17=91 files, 0 c	dir.; 9 🍸
🔜 X-Ways Forensics 🗾	Filename	Ext. P	ath	Size A	Created	a de la composition de	Modified	Accessed	Attr.	1st cluster	ID	Comment	
- <u>□</u> \	0,1020,299484,00[1].jpg	ipg \F	Pictures\0003	2.1 KB	03.05.2004	17:17:56	05.04.2004	12.05.2005	A	25395	382		
E WIFS Abused.e01	Private.jpg	ipg \F	Pictures\0001	6.2 KB	03.05.2004	17:17:58	10.09.1997	12.05.2005	A	31337	511		
	350de005.jpg	ipg \F	Pictures\0003	7.1 KB	03.05.2004	17:17:56	03.05.2004	12.05.2005	Н	25465	385		
Signets	makeup4.jpg	ipg \F	Pictures\0003	14.4 KB	03.05.2004	17:17:56	03.05.2004	. 13.05.2004	A	26491	403		
	e la necklace1.jpg	ipg \F	Pictures\0003	14.6 KB	03.05.2004	17:17:56	03.05.2004	. 12.05.2005	A	26449	399	Here	
Pathunknown	e in new-york-9400020.jpg	ipg \F	Pictures\0003	18.6 KB	03.05.2004	17:17:56	24.03.2004	12.05.2005	A	26465	401	you can	_
	Nine Planets ipeg	ipeg \F	Pictures\0001	20.6 KB	03.05.2004	17:17:58	30.04.2004	12.05.2005	A	31032	501	add	_
Excond E	e ewelry.jpg	ipg \F	Pictures\0003	20.7 KB	03.05.2004	17:17:56	03.05.2004	13.05.2004	A	26383	397	comments.	_
Documents and Settings	Neo & Trinity 1.jpg	ipg \F	Pictures\0001	26.3 KB	03.05.2004	17:17:58	26.06.1999	. 17.05.2005	A	30966	499		
🕀 🧰 Microsoft Works	Patrick Stewart 2.jpeg	Ipeg \F	rictures\0001	27.2 KB	03.05.2004	17:17:58	24.02.1997	. 12.05.2005	A	31169	506		_
🖹 🖂 Pictures	I ripod 3.jpg	ipg \F	Pictures\UUU2	29.2 KB	J3.U5.2UU4	17:17:57	30.04.2004	13.01.2005	A	29261	457		
	Inpod Lpg	ipg M	Pictures\0002	29.3 KB	J3.U5.2UU4		View	P	A	29246	455		
	makeup3.jpg	ipg \t	Pictures\0003	32.0 KB	03.05.2004	17:17:	External Prog	grams 🕨	A	26475	402		-
0003	Zhang Ziyi 40.jpg	IPG M	Pictures\0001	32.1 KB	03.05.2004	17:17	Deservedore	P	A	31479	517		-
RECYCLER	sparpreis50.gir	git M	Pictures\0003	34.2 KB	03.05.2004	17:17	Recover/Cop	y	A	26631	408		_
System Volume Information	McLoy.jpeg	Ipeg \r	Pictures\UUU1	35.5 KB	03.05.2004	170170	Edit comment	-	A	30787	494		-
	Patrick Stewart 5.jpg	ipg \r	Pictures\UUU1	36.5 KB	03.05.2004	17:17:	Add To Activ	e Case 🚦	A	31185	507		
Jignets	Spock I.lpg	Ipg vr	-ictures\0001	36.9 KB	03.05.2004	17:17:	Add to	• E	A	31409	514		
	Sectors Preview Gallery	Caler	ndar Leger	nd			Tag						
Rath upknown		Cart March		-			Hide		-	(25) TA		100	-
	· 25	and the				-	Position			Q- 5	100	1.32	
bin bin			No.				1 OSIGOIT	·				-13 I	
😥 🧰 boot		0 <u>E</u>			1 1		Logical Searc	h					
cdrom					_		Create Hash	Set					
😥 💼 dev 📃		Arres to		an ar ar	McCoy	ipeg	Print						
🗈 🧰 etc				a 19,7 (J. 19)	Extens	ion: jp	Open				-	Ter	
				2	35.5 K	Ball 🛄				6			
				8 : I :: I, I :	E Contap	(filo)				S& 10			
		a 44 1	(11 a) 10			0							
lost+round	And the second s		Corel	- Constanting	1			Mist.jpeg	inea				
mnt C						100 16	A STREET	53.9 KB	Ibed 2	Section and	3		
none A oot		1 S 1		<u>.</u>		Sur Par		(corrupt file	e) 🔛	1- 1-	÷	•	-1
			L		10.6.34	Ser and					1		-

Figure 5: X-Ways UI (X-ways, 2017b).

**Encase**. Encase is a famous forensic tool with the combination of many tools in the field of digital forensics. It was first started in 1988. It has been the best in the business and was awarded best forensic toolkit for seven years continuously. It acquires data from the disk level, from a variety of devices, it has a feature to complete investigate at the disk level (Encase, 2017).

🖬 EnCase Enterprise Training													
💷 💌 🚺 Case (new) 🔻 🖏 View 🔻 🎲 Tools 🔻 🙀 Enterprise 💌 😤 Add Evidence 💌 🔞 💌													
🛅 Home 🖉 Evidence 🛛 🗔 Case Analyzer 🗙													
tome € Refresh v													
🖂 Case Analyzer 🛪 🖂 Case 🛪 📑 🗳													
🔾 🕄 🖾 Manage Saved Reports 🚵 Unavailable Reports (ﷺ Target Constraint 🔀 Clear Constraint													
🕒 Selected 0/30 🍽 🔞 🚽 👘 Selected 0/608 🕼 Constraint 🔀 Clear Constraint 🖤 Save Selected 🚫 Bookmark Selected @ About													
Reports Accounts and Users		Target	Local Port	Local IP Address	Remote Port	Remote IP Address	Protocol	Process ID	Parent Process ID	Process Name	State	Instance Name	^
File Activity	9	192.168.177.188.0	49380	192.168.177.188	1000	172.21.12.121	TCP	2572	3424	javaw.exe	SYN_SENT	javaw.exe	
Open Files	10	192.168.177.188.0	49384	192.168.177.188	1000	172.21.12.121	TCP	2572	3424	javaw.exe	SYN_SENT	javaw.exe	=
A B Network	11	192.168.177.188.0	0		0		NONE	1992	0	enstart.exe	UNKNOWN	enstart	
ARP	12	192.168.177.188.0	0		0		NONE	1992	604	enstart.exe	UNKNOWN	enstart.exe	
DNS	13	192.168.177.188.0	0		0		NONE	1992	0	enstart.exe	UNKNOWN	enstart	
IP Gateway Pairs	14	192.168.177.188.0	0		0		NONE	1992	604	enstart.exe	UNKNOWN	enstart.exe	
Network Interfaces - Span	15	192.168.177.188.0	135		0		TCP	804	604	svchost.exe	LISTENING	svchost.exe	
Open Ports	16	192.168.177.188.0	135		0		TCP6	804	604	svchost.exe	LISTENING	svchost.exe	
Open Ports By DLL	17	192.168.177.188.0	135		0		TCP	804	604	svchost.exe	LISTENING	svchost.exe	
Open Ports No Process	18	192.168.177.188.0	135		0		TCP6	804	604	svchost.exe	LISTENING	svchost.exe	
Routes	19	192.168.177.188.0	500		0		UDP	964	0	svchost.exe	UNKNOWN	Application Information	
Derating System	20	192.168.177.188.0	500		0		UDP	964	0	svchost.exe	UNKNOWN	Application Management	
⊳} Software Usage & Autorun	21	192.168.177.188.0	500		0		UDP	964	0	svchost.exe	UNKNOWN	Background Intelligent Tran	nsf
▶— 🛛 🕌 System Changes	22	192.168.177.188.0	500		0		UDP	964	0	svchost.exe	UNKNOWN	Computer Browser	
	23	192.168.177.188.0	500		0		UDP	964	0	svchost.exe	UNKNOWN	Group Policy Client	
	24	192.168.177.188.0	500		0		UDP	964	0	svchost.exe	UNKNOWN	IKE and AuthIP IPsec Keying	м
	25	192.168.177.188-0	500		0		UDP	964	0	svchost.exe	UNKNOWN	IP Helper	
	26	192.168.177.188.0	500		0		UDP	964	0	svchost.exe	UNKNOWN	Secondary Logon	
	27	192.168.177.188.0	500		0		UDP	964	0	svchost.exe	UNKNOWN	Server	
	28	192.168.177.188.0	500		0		UDP	964	0	svchost.exe	UNKNOWN	Shell Hardware Detection	-
•				m					-				P.
✓ III → First 4 → 1 → 2 → 3 → 4 → Last (4) → Go to Page 2 Change Page Size → Show All													
Selected Report Title: "Open Ports"													

Figure 6: Encase UI (Mizota, 2015).

#### **Evolution of SSD**

The Evolution of SSD started nearly 40 years back where it was called Solid State Disk.

First SSD was built in 1976 with a name Bulk Core. It was 19 inches wide and 15.75 inches tall,

1 TB of this would cost about \$152 billion in current day currency (Edwards, 2012).



Figure 7: SSD internal structure (Amazon.ca, 2017b).

In 1978, STC (Storage Technology Corporation) introduced 4305 cabinet which is 45 MB storage facility. It has dual controller cards which would cost around \$400000 and \$1.5 Million equivalent to present-day currency. It was 52% cheaper cost compared to IBM drum storage (Edwards, 2012).

In 1979, Intel introduced 1 MB bubble memory chip which is called as 7110. This cost around \$895 for 128KB. In 1982, Apple 2 ram was launched Nolan Bushnell's toy company Axlon, it would cost about \$1395 which can store up to 320KB, as the data in this device is stored in RAM chips a battery is included which can run on a 3hour rechargeable battery (Edwards, 2012).

Later in 1982, a new issue advertisement was given on Byte magazine with 256KB RAM developed which costs around \$800. Axlon was a company more focused on developing SSD for computer, in 1983 it developed a 1 MB storage which developed based on 256KB configuration costs around \$1095 (Edwards, 2012).

In 1988, a first flash drive was developed by Digipro, it could hold up to 16MB of data, it came out in 1990 in 4 different models with the capacity of 2MB, 4MB, 6MB, and 8 MB which cost around \$5000. In 1989M-systems an Israeli based company developed first flash drive, but it did not release it till 1995 which made the flash disk from Digipro world's first SSD. Even after 1990, the flash memory was still rare and costly, they are limited to servers where data access speed is high. The series of 5.25-inch SCSI-based drives shipped in capacities of 107MB (\$13,999) to 428MB (\$47,099). The faster series offered capacities from 120MB (\$40,000) to 1GB (\$135,000) (Edwards, 2012).

In 1996, Newer Tech Dart Drive and ATTO Silicon Drive 2 which could store up to 2.6GB of data would cost in thousands of dollars as they were intended for the high-end use only where they are used only when the data processing time should be less. As we discussed earlier all the SSD's were equipped with a battery not to lose data when there is a power loss. This device is called as the workstation SSD which is much faster compared to nowadays hard drives with 0.02ms of access time (Edwards, 2012).

In 1995, M-Systems introduced fastest flash drive called Fast Flash Disk, it is small with 3.5 inches, it comes with memory accommodation of 16MB to 896MB and costs around \$10000 per a drive, as they are costly it is mostly used in military and aeronautical applications, for the next 10 years M-Systems continuously developed SSD's with more capacity, high speed, and less cost (Edwards, 2012).

Finally, in 2003 the cheaper versions of flash drives were started produced by the companies. Transcend introduced a parallel ATA where it is much smaller in size compared to traditional hard drives, they can accommodate data from 16MB to 512MB. They are usually used in digital cameras which would cost up to \$50.



#### Figure 8: V-NAND SSD (Newegg, 2017).

In 2006, Samsung first came into SSDs market with first mass-market flash, which is 2.5 inch in size and would cost up to \$699 for 32GB memory capacity. SanDisk followed in 2007 with the same configuration in 2007. The SSDs were rewritable, unlike flash drives at that time. Pushing the limits SSD technology has greatly emerged and hard drives usage has been reduced and in 2009 Fusion IODrive Duo was introduced with a capacity of 126GB to 1.2TB with a cost range starting from \$5950. It has a speed of 1.5GB per second (Edwards, 2012). Today's consumer SSDs keep getting faster and cheaper thanks to new flash chips and higher-speed SATA interfaces. For example, the 160GB member of the Intel 320 SSD series, shown here, currently retails for about \$320 and offers sustained read speeds of 270 MBPS (Edwards, 2012). In 2008, almost 100 companies have started producing SSDs, EMC, Adtron, Seagate, OCZ, Silicon Systems have started producing SSDs with different capacities and access time (Kerekes, 2017).

Year		1998	1999	2000	2001	2002	2003	2004	2005	2006 2	007 200	08 200	9 2010	2011	
NAND design tool		250nm		) 160nm		130nm		90nm 6x nm		k nm	5x nm 4x	nm 3x	) 3x nm 2x nm 1x nm		
NAND block size	SLC			16kByte				128kByte		/te	> 256	kByte	e 512kByte		
	MLC								256kE	Byte	> 512	Byte	► 1M	/Byte	
	Bus							XR		RA6	RA7	RA8			
GBDriver	ATA			SA	SA2	A RA2	RA3		RA4			1			
	SATA										RS	RS	2	RS3	
Capacitance	CF					~2		GB ~4G		√4GB (~8GB (~		-16GB ~		-32GB	
	SSD									~8	GB ~16	GB	~64GB	~128GB	
GBDriver ECC capability								2bit		4bit	8bit	1	15bit	44bit	
NAND Endurance					300,00	00 times		> 100,000		00 times		- 50,	000 times	$\geq$	
NAND Ret	tention								10 years						

#### Evolution of TDK's memory controller IC "GBDriver"

Figure 9: Evolution of SSD (ESSD Embedded, 2017)

In 2017, Crossbar has announced that it is working on an 8MB ReRAM, Intel also started working on the future of the storage devices and day by day all the personal computers and laptops have been started equipped with the modern day SSDs with much more capacity and faster access speed. SSD is now available in many capacities ranging to 16TB and it is said to be increased to 40Tb by 2017 (Kerekes, 2017).

The capacity of SSD is said to be increased to 128TB by the end of 2018 and will continue growing in future thereafter. SSD has made a great revolution in both size and storage capacity in the digital world (Humphries, 2017).



Figure 10: Usage of SSD and HHD comparison (Mellor, 2013).

As CPU performance comes into consideration SSD predominantly out runs hard drives. The hard drives in a system can be easily replaced with an SSD if speed is not a concern and n code processing to be done then hard drives do the same work as of SSD. Noise is completely reduced as there are no moving parts involved in the SSDs. There are no magnets involved in the SSD which will completely remove the disadvantage of the magnetism, as the running disks are eliminated in the SSD, heat production is completely reduced which helps in increasing the lifespan of the disk and reliability. Due to the reduction in the heat, it also helps to reduce the damage of the system part as well.

#### **Advantages of SSD**

SSD has more advantages when compared to Hard drives, some of them are listed below:

- 1. Access Time: Access time of an SSD is much more efficient when compared to hard drive as it is equipped with the memory cells as in case of a Ram it is faster comparatively. An SSD has access speeds of 35 to 100 microseconds, which is nearly 100 times faster. This faster access speed means programs can run more quickly, which is very significant, especially for programs that access large amounts of data often like your operating system (Computer Hope, 2017a).
- 2. Price: The price of an SSD is relatively high due to the memory components used in the SSD. The relatively high price of an SSD is the reason we do not find higher capacity storage device in modern computers. The storage capacity of an SSD equipped system is in GB when it is in TB for a hard drive equipped systems, but the storage done in them are relatively same (Computer Hope, 2017a).
- **3. Reliability:** As we know that the SSD does not have any moving parts we can say that it is more reliable due to the other advantages of an SSD like capacity, noise, heat, and magnetism (Computer Hope, 2017a).
- **4. Capacity:** The price range of the SSD is relatively high when compared to the HDD but relatively 512GB of memory is sufficient for the user when compared to 1TB of a hard drive (Computer Hope, 2017a).
- **5. Power:** The SSD uses less power when compared to HDD as the utilization of power for the extra components are eliminated in SSD, this means that it utilizes less power which in turn reduces the power bills and the battery life of the system will be improved and can be utilized for another purpose (Computer Hope, 2017a).

- 6. Noise: With no moving parts SSD generates no noise. There is no disk running to access data and no pointers are involved which makes reduces the noise concept.
- 7. Size: Size of an SSD is less compared to hard drive making them portable and due to the reduction in the part it is relatively small. It is available in different sizes and shapes. SSD is available in 2.5", 1.8", and 1.0", increasing the available space available in a computer, especially a desktop or a server (Computer Hope, 2017a).
- Heat: Because there are no moving parts and due to the nature of flash memory, the SSD generates less heat, helping to increase its lifespan and reliability (Computer Hope, 2017a).
- 9. Magnetism: SSD is not affected by magnetism. As SSD do not rely on the magnetic disks and pointer to write data there are no concepts of magnetism in SSD (Computer Hope, 2017a).

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

#### Hard Disk Drives

A general computer has different storages spaces or devices among which Hard Disk has the most memory space. It is considered as the main and the largest storage space in a physical computer. Most important data are stored in Hard disks such as the Operating system, drivers, system related files etc. As we know the program files reside in C drive which is nothing but the Hard Disk in general (Fisher, 2017).





There are many competitors in HDD manufacturing among them Seagate, Western digital, Samsung, Kingston etc. are some popular manufacturers. It comes in different sizes and shapes. Some are mounted inside CPU or Laptops and some can be connected externally. The

cables used to connect the motherboard to the Hard disk are identified as two types based on the variant SATA and PATA (Fisher, 2017).

How data is read in Hard Drive. A Disk Controller is used to read and write data to the Hard Drives. It will instruct the Hard drive how to perform an operation like reading a file, writing to a file, accessing a file location. Once FAT of a hard drive is determined then the disk controller will instruct the actuator to align the read or write head by moving the read write arm. Files are not stored in sequential memory locations and are scattered in different places of hard disk thus the actuator and disk controller help in accessing the files (Computer Hope, 2017b).

Data is stored in hard drives magnetically which means it is stored and then retrieved using magnetic disks and magnetic polarities.



Figure 12: Hard disk internal structure (Evan Amos, 2017).

#### **Solid State Drives**

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

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

Cache is the innermost memory unit. Cache is used as a sort of playground for doing all calculation and procedures as the computer operates. The data access is instantaneous, electrical pathways to the cache are the shortest because the cache is mandatory. Memory is the middle ground for computer known as RAM, Random Access Memory. RAM is the place where information is being stored related to processes running on your machine and active programs. Access to the memory is slow when compared to that of cache. A hard disk is a place where
everything is being stored for performance. Hard disk stores all our configuration files, programs, music files, documents, and more. When a file is needed to be accessed or when we need to run a program it needs to be loaded from the hard disk and then into the memory (Evans, 2012).

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

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



Figure 13: Solid state drives (Ngo., 2013).

NAND flash memory. Modern Solid State Drives use NAND flash memory which is an integrated circuit designed for storing information. Enterprise Solid State Drives use a single-layer cell NAND, i.e., SLC NAND, whereas consumer grade SSD's use a multilayer cell NAND. The former is fast and would last longer than the latter, however, it is more expensive. As these are not magnetic platters, writing to an SSD occurs when the controller programs the memory cells for storing the information. The memory shell would store voltage and would be either on 1 or 0 state, which allows them to store data in binary form. Come to reality writing data to an SSD is a complicated process. However, reading data is relatively simple because the controller doesn't have a lot to work to do (Masuoka, 1987).

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

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

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

### Hardware and Software Requirements

- FTK Imager
- FTK Tool
- Open Computer Forensics Architecture
- SSD Lexar by Micron, 512GB
- Interface USD 3.0
- MPN LRWSSD512SBC
- Model LRWSSD512SBC

- Laptop HP Pavilion
- OS Windows 10 version 10.0.14393
- OS build 14393.953
- Processor Intel<sup>®</sup> Core<sup>™</sup> i5 5200U CPU @ 2.20GHZ 2.20GHZ
- Installed RAM 4.00 GB
- System Type 64-bit operating system, X64-based Processor

## **Summary**

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

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

#### Introduction

In this chapter, we will prepare an evidence file by collecting data and key words to search them, we will discuss how this data is being collected and stored in evidence folders, total number of original files that we pass to SSD and HDD. We will also discuss how data is being stored in both devices, how the images of evidence files passed to the drives are created. We will discuss how FTK and Autopsy are being used for creating the image files from the drives, how HD Shredder is used to format the drives and analyze the evidence folder when it is passed through FTK Toolkit and Autopsy.

#### **Data Presentation**

The evidence is collected in the form of junk data which is the combination of word documents, excel documents, notes, images and actual evidence. Actual evidences that we are investigating on includes cars, farmhouses, phones, medicines and laptops. Evidences are passed with different combinations into each drive multiple times and deleted before creating image files.

encefiles   evidencefiles		✓ <sup>€</sup> → Search ev	idencefiles		Q
Share with 🔻 New folder					?
*	Date modified	Туре	Size		
	10/18/2017 11:15	File folder			
n House	10/18/2017 11:15	File folder			
tops	10/18/2017 11:15	File folder			
licines	10/18/2017 11:15	File folder			
nes	10/18/2017 11:15	File folder			
	Share with  New folder Normality New folder Normality No	Share with ▼         New folder           Date modified         10/18/2017 11:15           In House         10/18/2017 11:15           tops         10/18/2017 11:15           dicines         10/18/2017 11:15           nes         10/18/2017 11:15	Share with ▼     New folder       Date modified     Type       10/18/2017 11:15     File folder       10/18/2017 11:15     File folder       tops     10/18/2017 11:15     File folder       flicines     10/18/2017 11:15     File folder       nes     10/18/2017 11:15     File folder	Share with ▼     New folder       Date modified     Type       10/18/2017 11:15     File folder       10/18/2017 11:15     File folder       tops     10/18/2017 11:15       10/18/2017 11:15     File folder       iticines     10/18/2017 11:15       nes     10/18/2017 11:15	Share with ▼       New folder       Image: Constraint of the state of th

Figure 14: Evidence folders.

Favorites Desktop Downloads Recent Places QA	Carl	Car2	Car3	Car5	Car6	Car7
Libraries Documents Music Pictures Videos	Car8	Car9	Car10	Carl4		

Figure 15: Evidence car folder.



Figure 16: Evidence medicine folder.



Figure 17: Evidence farm house folder.



Figure 18: Evidence phone folder.





Evidence files are now passes to both the drives by deleting them multiple times with various combinations to get number of hits for each key word search in FTK and Autopsy, these evidences files were created and a Junk File folder which has multiple Word Documents, Excel Sheets, PDF Files, and Images is passed along with the actual evidences. The sample project folder that we are investigating contains around 80 GB of data



Figure 20: Combined file size of the evidence, evidence thrashers, and junk file.

Both SSD and HDD are wiped using HD Shredder. This will wipe all the data from the

drives.



Figure 21: Installation of HD shredder.



Figure 22: Running HD shredder.

HDShredder free Edition -	a x	HDShredder Free Edition	a x
HDShredder 4	- <b>E</b>	HDShredder 4.	-
Deletion mode 😰 Drive Medium not selected Deletion method - not selected Options not selected		Deletion mode Drive Medium not selected Deletion method not selected Options not selected	
Prive      It IDE 244,519 MB - Sanchik 74005 2.3 7MM 25608      THE 244,519 MB - Bur Blim IL      It IDE 363,870 MB - Bur Blim IL      It IDE 364,870 MB -	0	Drive  II. DC. 244,109 Nb KTVH035649744KW0K.  IZ. USB. 448,307 Nb KFF-53D  Defails  Channel(Svar. Usb. Chances in the sectable of the se	00
( Back	Next )	4 Back	Next>

Figure 23: Detecting both the drive on two different laptops.

Once the process is initiated it took around 3 hours for the drives to be completely wiped using the HD Shredder software.



Figure 24: Drive wiping process at random intervals in HDD and SSD.



Figure 25: Successful completion of disk wiping using HD shredder.

All the evidence thrasher files are passed to both HDD and SSD at different

combinations. The following figure illustrates the different combinations that are being used.



Figure 26: Passing evidence.

Image     Image       File     Home       Share     View       Manage	File     Home     Share     View     Manage          ←        →        ★        →        Yeise
<ul> <li>← → ✓ ↑ → This PC &gt; New Volume (D.)</li> <li>Posktop ★</li> <li>Downloads ★</li> <li>Documents ★</li> </ul>	<ul> <li>Quick access</li> <li>Desktop</li> <li>Downloads</li> <li>Documents</li> <li>Pictures</li> </ul>

Figure 27: Passing Evidence 1, Evidence 2.

Image: Image	Tools New Volume (D:)	↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓	Drive Tools New Volume (E:) View Manage
<ul> <li>← → · ↑ → This PC &gt; New Volu</li> <li>← → · ↑ → This PC &gt; New Volu</li> <li>↓ Cuick access</li> <li>↓ Evidence</li> <li>↓ Evidence</li> <li>↓ Evidence</li> <li>↓ evidence</li> <li>↓ Junk</li> </ul>	ume (D:) te Trasher 1 te Trasher 3 tes	<ul> <li>← → × ↑ → This PC</li> <li>✓ Quick access</li> <li>Desktop</li> <li>Downloads</li> <li>Documents</li> <li>Pictures</li> </ul>	<ul> <li>New Volume (E:)</li> <li>Evidence Trasher 1</li> <li>Evidence Trasher 3</li> <li>evidences</li> <li>Junk</li> </ul>

Figure 28: Passing Evidence 1, Evidence 3.

↓     ↓     ↓     Drive Tools     New Volume (D:)       File     Home     Share     View     Manage	Image: Price File     Image: Price File     Drive Tools     New Volume (E:)       File     Home     Share     View     Manage
<ul> <li>← → &lt; ↑ </li> <li>→ This PC &gt; New Volume (D:)</li> <li>✓ Quick access</li> <li>▲ Desktop</li> <li>♦ Downloads</li> <li>♦ Documents</li> </ul>	<ul> <li>This PC &gt; New Volume (E:)</li> <li>Quick access</li> <li>Desktop</li> <li>Downloads</li> <li>Documents</li> <li>Pictures</li> <li>Pictures</li> <li>New Volume (E:)</li> <li>Evidence Trasher 1</li> <li>Evidence Trasher 4</li> <li>evidences</li> <li>Junk</li> </ul>

Figure 29: Passing Evidence 1, Evidence 4.

Image     Image       File     Home       Share     View       Manage	✓ I ✓ I ✓ I ✓ Drive Tools New Volume (E:)           File         Home         Share         View         Manage
<ul> <li>← → &lt; ↑ → This PC &gt; New Volume (D:)</li> <li>Documents </li> <li>Pictures </li> <li>Pictures </li> <li>Cloud Photo: </li> <li>Ficloud Drive </li> <li>Icloud Drive </li> <li>Junk</li> </ul>	<ul> <li>← → · ↑ → This PC &gt; New Volume (E:)</li> <li>✓ ★ Quick access</li> <li>▶ Desktop</li> <li>▶ Downloads</li> <li>▶ Downloads</li> <li>▶ Documents</li> <li>▶ Pictures</li> <li>★</li> </ul>

Figure 30: Passing Evidence 2, Evidence 3.

🥪 📝 📙 🕫 🛛	Drive Tools	New Volume (D:)	🥪   🗹 📕 =		Drive Tools	New Volume (E:)
File Home Share View	v Manage		File Home	Share View	Manage	
$\leftarrow$ $\rightarrow$ $\checkmark$ $\uparrow$ $\checkmark$ $\Rightarrow$ This PC $\rightarrow$	New Volume (I	D:)	← → • ↑ •	> This PC > N	ew Volume (I	E:)
Documents 🖈 ^	Evidence Trac	har 2	🔹 Quick access		📕 Eviden	ce Trasher 2
E Pictures 🖈	Evidence Tras	her 4	Desktop	*	Eviden	ce Trasher 4
🌸 iCloud Photo: 🖈	Junk		Downloads	*	Julik	
i Cloud Drive			📔 Documents	*		

Figure 31: Passing Evidence 2, Evidence 4.



Figure 32: Passing Evidence 2, Evidence 4.

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

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

Select Source ×	,
Please Select the Source Evidence Type    Physical Drive   Logical Drive  Image File   Contents of a Folder  (logical file-level analysis only; excludes deleted, unallocated, etc.)  Contents of a Police (multiple CD/(D))	
Service (Inductive Objecto)       < Back	

Figure 33: Selecting the source evidence.

As we are selecting contents of a folder it does not include any metadata, deleted files,

unallocated space, etc. in the image created. Following is the warning displayed.



Figure 34: Creating the image of a folder.

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

	Select File	×
Ev	idence Source Selection	1
	Please enter the source path:	
	C:\Users\yash\Desktop\Car	
	Browse	
	< Back Finish Cancel Help	

Figure 35: Selecting the source path.

Data is filled in all required fields for Case Number, evidence number, examiner name

before moving to next step.

	Create Image	×
	Evidence Item Information	×
Case Number:	defence	
Evidence Number:	1	
Unique Description:	ltkdefence	
Examinent	yaah	
Notes:		
	Cancel Help	
	Start Cancel	

Figure 36: Assigning name for unique identification.

The image source is selected from the drive and image file destination is selected for storing them

	Create Image		×
Image Source			_
C:\Users\premnath\Des	sktop\Car		
L	Starting Evidence Number:	1	
Image Destination(s)			
C:\Users\premnath\One	Drive\eviednce [Logical image]		
Add	Edit	Remove	
	Add Overflow Location		
			_
Verify images after the	ey are created Precalculat	te Progress Statistics	
Create directory listing	s of all files in the image after th	ey are created	
	Start Cancel	1	
_	Curter		

Figure 37: Assigning image destination.

Fragmentation size is given to create multiple images of the evidence file and then click

on finish to start creating image files

Create Image	×
Select Image Destination	×
Image Destination Folder	
C:\Users\yash\Desktop Browse	
Image Filename (Excluding Extension)	
eviednce	
Image Fragment Size (MB) [1500 For Raw, E01, and AFF formats: 0 - do not fragment	
Compression (0=None, 1=Fastest,, 9=Smallest)  6	
Use AD Encryption	
Filter by File Owner	
< Back Finish Cancel Help	
Start: Cancel	

Figure 38: Selecting the fragmentation size.

The image creation can be seen in the below image as the image files for the selected folder or evidence.

	Creating Image – 🗆 🗙
Image Source:	C:\Users\premnath\Desktop\Car
Destination:	C:\Users\premnath\OneDrive\eviednce
Status:	Image created successfully
Progress	
Elap Esti	mated time left:
Image Summar	y Close

Figure 39: Processing of image creation.

Once the image for the evidence folder is created the below data is displayed which

ensures successful creation. Hash number is created for the image file to make sure no

evidences are tampered in future

Image Summar	y 💌
Created By AccessData® FTK® Imager 4.1.1.1	^
Case Information: Acquired using: ADI4.1.1.1 Case Number: defence Evidence Number: 1 Unique Description: fitxdefence	
Examiner: yash Notes:	
Information for C:\Users\premnath\OneDrive\ev [Computed Hashes] MD5 checksum: 20dca89bca6885f%e6234faeb SHA1 checksum: 4091015da8cf13c10bbdf97ae	iednoe.ad1: 76edf50 23763d6cf27bc7cd
Image information: Acquisition started: Wed Oct 18 18:58:58 2017 Acquisition finished: Wed Oct 18 18:58:58 2017 Segment list: C:\Users\premnath\OneDrive\eviednce.ad1	7
Image Verification Results: Verification started: Wed Oct 18 18:58:58 2017	, ,
<	>
	ок

Figure 40: Verifying results of the image created.

All the details that we provided are shown in this image this is summary of the image

file

Image Summary	×
Created By AccessData® FTK® Imager 4.1.1.1 Case Information: Acquired using: AD14.1.1.1 Case Number: defence Evidence Number: 1 Unique Description: ftkdefence Examiner: yash Notes:	^
Information for C: \Users\premnath\OneDrive\eviednce.ad1: [Computed Hashes] MD5 checksum: 20dca89bca6885f4e6234faeb76edf50 SHA1 checksum: 4091015da8cf13c10bbdf97ae3763d6cf27bc7cd Image information:	
Acquisition started: Wed Oct 18 18:58:58 2017 Acquisition finished: Wed Oct 18 18:58:58 2017 Segment list: C:\Users\premnath\OneDrive\eviednce.ad1 Image Verification Results:	2
Verification started: Wed Oct 18 18:58:58 2017	× ~
	к

Figure 41: Image summary for image.

On successful creation of the image the files are stored in the location we specified. We have chosen desktop as primary location during image creation, so all the image files created in the process are stored on to desktop.

Name	Date modified	Туре	Size
🌗 Car	10/18/2017 11:15	File folder	
🌗 Farm House	10/18/2017 11:15	File folder	
퉬 Laptops	10/18/2017 11:15	File folder	
Image:	10/18/2017 11:15	File folder	
퉬 phones	10/18/2017 11:15	File folder	
eviednce.ad1	10/18/2017 6:59 PM	AD1 File	192 KB

Figure 42: Image of evidence folder.

## **Data Analysis**

After the creation of image files of evidences, the images are analyzed to retrieve results. The image files are analyzed using two forensic tools FTK Toolkit and Autopsy.

Analyzing the image of evidence folder using FTK. To analyze the image created using the FTK Imager, we will use FTK toolkit. We need to provide the required fields before starting analysis. Case Number, examiner name, path of the image file and case folder is provided.

In the next step, we need to enter personal details of the investigator who is analyzing the image like: Which company, Name of the investigator, Address, phone number, and Email address. Click on next to proceed further.

e following information	n will appear on the Case Information page of the report:	
Agency/Company:	Saint Cloud State University	
Examiner's Name	Shiva ~	
Address:	10480 Maya Linda Road G209, San Diego, ca 9216	
Phone:	320-339-3935 Fax:	
E-Mail:	ssmarupudi@stcloudstate.edu	
Comments:		

Figure 43: Filling personal details of investigator (Marupudi, 2017).

In the next step, we now need to select the image file that need to be analyzed. As we are analyzing an entire drive we need to select Acquired Image of the Drive radio button and click on continue.

Add Evidence to Case			$\times$
Any number of evidence items of Acquired image of drive: Local drive: Folder: Individual File: The default refinements can also be folders. To make these further ref Add Evidence	Add Evidence         In be added to the case. There are several types of evide         Several formats supported; can be an image of a logical         Can be a logical or physical drive         Adds all files in the specified folder, including contents of         Adds. These refinements can include the exclusion of data         Add Evidence to Case         Add Evidence to Add to Case         Octated Drive         Contents of a Folder         Individual File	ence items: or physical drive f subfolders ded as acquired it evidence item, an ite/size ranges, a Tefine Evidence efine Evidence Time Zone	mages. d additional s well as specific - Advanced Advanced Comment
	< Back	Next >	Cancel

Figure 44: Adding image file to FTK toolkit.

Image file from the system is selected using the browse option and click on OK.

		Add Eviden	ce			]	Add Evidence		
An A Open				×		Any number of evidence ite	ems can be added to the case. There are several types of evidence it	ems:	
Copen Look in: The Quick access Desktop Libraries	Desktop	m nentation oft Word Document B c (mane ad)	v 🧿 🎓 🛤 🕶	×	fic	An number of evidence is Acquared image of Local drive: Folder: Individual File: The default enterents can a folders. To make these ful Add Evidence Display Name	Imis can be added to the case. There are several types of evidence in Evidence Information × Evidence Location:  C:VJ.sert/shiva/Desktop/Evidence Image.ad1 Evidence Diplog Name:  Evidence Diplog Name:  Evidence Unit Comment:  Comment:	ems: ical drive ters scquired i tem, an ranges, a Evidence idence Zone	mages. d additional s well as specific - Advanced Comment
This PC	File name: Files of type:	er mage.ad1 oft Excel Comma Sep Evidence Image All Files (".")	× ×	V Open Cancel			Local Evidence Time Zone: Choose time zone for evidence	Ļ	
			< Back Next >	Cancel			< Back	lext >	Cancel

Figure 45: Adding image file to analyze (Marupudi, 2017).

In the next step, the details of the image file selected is displayed with next button and add evidence button.

dd Evidence to Case						×	Case Summary			
Any number of evidence te Acquired image of Local drive: Folder: The default drive the default drive the default drive the default drive the default drive t	ms can be added to th drive: Several formats Can be a logical Adda af lines in t dda as angel fil nos a set previously, car os a set previously, c	Add Evic e case. There supported, car or physical difference execution of the specified for execution of the specified for the average of the specified for memory and the specified for the spe	Jence are several type to be an image due der, including o independently including independently including independently including accessible Accessible	s of eviden f a logical or ontents of s uid be adde for each evid sion of date and press R Refined N	ce tems: physical drive ubfolders d ea acquired dence tem, ar dence tem, ar dence tem, ar dence Evidence Time Zone America/L	ndges. ndgdtional as well as specific - Advanced. Advanced.	Case Settin Case Sate Numb Proce	New Cas and the stand of the stand and the stand and the stand and the stand and	tabase, it restant 1 Yes Yes Yes Yes Yes Yes Yes Yes No No No	And the case-specific files will be stored.
							Press Press	"Back." If you wish to revi "Finish" to accept the cu	ew or chu rrent setti	ange your settings ngs and start processing the evidence

Figure 46: Evidence summary and add evidence (Marupudi, 2017).

Image is being processed.

C:\Users\shiva\De	sktop\Evidence Image.ad1		
Current File Item:			
Evidence Image\T	humbldx\_a\_6		
-Current File Item S	tatus	Total Process Status	
Action:	Indexing	Elapsed Time:	0.00:00:02
File Type:	Folder	Total Items Examined:	108
Item Size:	0	Total Items Added:	108
Progress:	100%	Total Items Indexed:	106

Figure 47: Extracting the files from image (Marupudi, 2017).

After the image file is processed it is analyzes using the FTK toolkit. Home page will look like below.

verview E	Explore	Graphics	E-Mail	Sear	rch	Bookmark.										
Evidence Items		ile Status	File Cate	gory			•	***	01 #1							
idence tems:	1 KFF Ale	t Files:	Documents:	0				Deco A two see	11 ET ET							
File Items	Bookma	rked tems:	Spreadsheets:	0												
al File berns: 2	202 Bad Ext	ension:	Databases:	1												
cked tems:	0 Encrypt	ed Files:	Graphics:	72												
checked items: 2	202 From E	nat.	Multimedia:	0												
ged Thumbnails:	0 Deleted	Files:	E-mai Message	s: 0												
or Thumbnails:	72 From R	cycle Bir:	Executables:	0												
red in: 2	202 Duplice	e terns:	Archives:	0												
ed Out.	0 OLE Su	stems:	Folders:	102												
Rered Filtered	d Flagged	Ignore:	Slack/Free Spa	Cer 0												
terns Actual Fa	les KFF lgn	orable:	Other Known 1	ype: 0												
Actual Fa B BB 42 C Evidence F Evi dence Image C.V	idence Path	orable: rved Files: orr Unfiltered Display Narr Evidence Ima	0 Other Known 1 2 Unknown Type e Identificati	ype: 0 27 III Evic Acco	dence Ty essData l	pe Added logic 6/15/20	012	Children	Descenda 02	nts 202	Investigator's shiva	Comr	nent			 
Actual Fa	idence Path	orable rved Files: orr Unfiltered Display Narr Evidence Ima	e Identificatio	ype: 0 27 III Marin - Evic Acce	dence Ty essData I	pe Added logic 6/15/20	012	Children	Descenda 02	nts 202	investigator's shiva	Comr	nent		 	 
Evidence Image	idence Path Users\shiva\	orable rved Files. 9 orr Unfiltered Display Nam Evidence Ima	Other Known 1 Unknown Type e Identificatio	ype 0 27 III Evic Acco	dence Ty essData I	pe Added logic 6/15/20	012	Children	Descenda 02	nts 202	Investigator's shiva	Comr	nent	1		
Evidence F Evidence Image C.V	idence Path	srable: rved Files: e orr Unfiltered Display Nam E vidence Ima	0 Other Known 1 9 Unknown Type e Identificatio	ype: 0 27 Im Acco	dence Ty essData I	pe Added logic 6/15/20	012	Children 40	Descenda 02	nts 202	Investigator's	Comr	nent			
Evidence F Evi ence Image C.V	Insers Shives	orable rved Files. orr Unfiltered Display Narr Evidence Ima	0 Other Known 1 Unknown Type e Identification	ype 0 27 m Evic Acco	dence Ty essData I	pe Added logic 6/15/20	072	Children 40	Descenda	nts 202	Investigator's shiva	Comr	sent		 	
Rems Actual Fi	ins KFF Ign Data Ci Cig D & idence Path Users\shiva\	vrable rved Files. orr Unfiltered Display Narr Evidence Ima	0 Other Known 1 Unknown Type e Identificatio	ype: 0 27 m _ Evic Acco	dence Ty	pe Added logic 6/15/20	072 17 10	Children 40	Descenda	nts 202	investigator's shive	Comr	nent			
Actual Fi BB 42 Evidence F Evi ence Image C.V	ies KFF (pr Data Cr Og D % idence Path Users/shiva/	srable: rved Files:	0 Other Known 1 Unknown Type e Identificatio	ype: 0 27 III MEvic Acco	dence Ty essData l	pe Added logic 6/15/20	orz	Children 40.	Descenda 02	nts 202	Investigator's	Comr	nent			
Ecos Actual Fi	idence Path Users\shiva\	rable rved Files. È orr Unfiltered Display Narr Evidence Ima	0 Other Known 1 0 Unknown Type e Identificatio	ype: 0 27 III III Acco	dence Ty essDate l	pe Added logic 6/15/20	972 17 10	40	Descenda	nts 202	Investigator's	Comr	sent			
tens Actual F8	ies RFF ign Data Cr Inter Cr I	reble rved Flex è orr Unfiltered Display Narr Evidence Ima	2 Other Known 2 Unknown Type ~ e Identificati #	ype 0 27 m Evic Acci	dence Ty essDate I	pe Added logic 6/15/20	972 17 10	Children 40	02 Descenda	nts 202	Investigator's	Come	sent			
Eens Actual Fa	ins RFF sp Data Cr Cata Cr Cat	rved Flex rved Flex orr Unfiltered Display Nam Evidence Ima	2 Other Known Unknown Type e Identificatio	ype 0 27 m – Evic Acci	dence Ty	pe Added logic 6/15/20	012	Children 40	Descenda 02	nts 202 :	Investigator's	Comr	nent			
Evidence F Evidence F Evidence F Evidence F	ies RFF ign Data Cr Cite Cr Cite Cr Citers Cather Users Shives	reble rved Flex e or Unfiltered Display Nem Evidence Ima	Other Known     Unknown Type     Unknown Type     e Identificatio	ype: 0 27 m Acco	dence Ty	pe Added logic 6/15/20	912 17 10.4	402	Descenda	nts 202	Investigator's	Comr	sent			
Rens Actual Fa	ins RFF sp Data Cr Cata Cr Cat	reble rved Flex orr Unfiltered Display Nam Evidence Ima	Other Known Type     Unknown Type  e Identificatio	ype 0 27 m un – Evic Acci	dence Ty	pe Added logic 6/15/20	012 17 10.4	Children 40	Descenda 02	nts 202	Investigator's	Comr	nent			

Figure 48: Home page of FTK toolkit (Marupudi, 2017).

In the evidence folder we created, we used 5 different keywords such as car, medicines,

laptops, farmhouse, and phones.

FTK has a feature to look at the image files which we passed. From the evidence folder,

we are aware that there is a picture of a farm house. Searching with a specific name is also

possible in FTK.

File Edit View Tools	Help							
Overview Expla	are Graphics	E-Mail	Search	Bookm	ark			
Evidence Hereit	File Status	E-India	Search	DOOKIN				
Evidence items	File Status	File Category		1 ( )	$\sim$	👾 🗠 🚓 🔛	🗄 📆 🙆 🎙	O] 🚑 ]
Evidence Items: 1	KFF Alert Files: 0	Documents:	0		,			
File Items	Bookmarked Items: 0	Spreadsheets:	0		1			
Total File Items: 202	Bad Extension: 0	Databases:	1					
Checked Items: 0	Encrypted Files: 0	Graphics:	72	and the second sec				
Unchecked Items: 202	From E-mail: 0	Multimedia:	0	CONTRACTOR OF				
Flagged Thumbnails: 0	Deleted Files: 0	E-mail Messages:	0		J			
Other Thumbnails: 72	From Recycle Bin: 0	Executables:	0					
Filtered In: 202	Duplicate Items: 0	Archives:	0					
Filtered Out: 0	OLE Subitems: 0	Folders:	102					
Unfiltered Filtered	Flagged Ignore: 0	Slack/Free Space:	0					
All Items Actual Files	KFF Ignorable: 0	Other Known Type:	0					
	Data Carved Files: 0	Unknown Type:	27					
	D & S3 orr Unditioned					017		
		~			$\sim$	DIZ		
File Name	Full Path			Recycle Bi	Ext	File Type	Category	Subject
🗖 🌆 2.jpg	Evidence Image	ThumbIdx\_2\2.jpg			ipg	JPEG/JFIF File	Graphic	
🗖 🌄 190.jpg	Evidence Image	Thumbldx\_a\_5\190.j	pg		ipg	JPEG/JFIF File	Graphic	
🗖 🌉 19.jpg	Evidence Image	ThumbIdx\_j\19.jpg			ipg	JPEG/JFIF File	Graphic	
🛛 🗖 🌄 18.jpg	Evidence Image	ThumbIdx\_i\18.jpg			ipg	JPEG/JFIF File	Graphic	
🗖 🌄 172.jpg	Evidence Image	ThumbIdx\_s\_4\172.jp	g		ipg	JPEG/JFIF File	Graphic	
🗖 🌄 171.jpg	Evidence Image	ThumbIdx\_r\_4\171.jp	g		ipg	JPEG/JFIF File	Graphic	
170.jpg	Evidence Image	ThumbIdx\_q\_4\170.j	pg		ipg	JPEG/JFIF File	Graphic	
17 ing	Evidence Image	Thumblds\_b\17 ina			ina	JPEGAIEIE Eile	Graphic	

Figure 49: Searching by the file names.

**Analyzing the image of evidence folder using autopsy**. The image file we created for the FTK is not compatible with Autopsy. Autopsy uses the E01 format where as FTK used Ad format.

To convert format, we use Forensic Imager tool. This involve following steps.



Figure 50: Home page of forensic imager.

We select second option to convert one format to another. Select option two and fill in

the required details.

ie Teh			
Select the image file to convert:			
Device Label B → 📌 JTmage Files	Size FS	Туре	
eviednc C: Users lyashwamth Downloads levidence files levidence.ad 1	1.46 GB File	AD1 Image	
			📇 Add Image
			🚫 Remove
Sector Range Starts Editor 0  End Sector 3077 999			
O Back Next O			

Figure 51: Selecting image to convert.

Source		
	C:\Users\yashwanth\Downloads\evidencefiles\evidencefiles\evidencefiles\evidencefiles\evidencefiles\evidencefiles	
Destination		
Image type: Dutnut filename:	e: Encase® (*e01) V File Segment Size (MB): 2000	
Ourput mename:	Hash Options: Calculate image MD5 Calculate image SHA1 Calculate image SHA25 Calculate SHA25 Calculate image SHA25 Calculate image SHA25 Calculate SHA25 Calculate image SHA25 Calculate SHA25 Calculat	
	Verify image hash after creation	
Details:		
Case Name:	e: 1	
Evidence Number	* 1	
Unique Description:		
Examiner:	sr: Vashwanth	
Notes:	x \$	
	G Back	Start 🌍

Next step, we will click on next button to select the format we want to convert.

Figure 52: Source of destination file forensic imager.

Next step, we will see the details of the image that is converted with the examiner details

and case number.

Details:       Source:       [C:\User\yashwamthDownload\vevidencefiles\vevidencefiles\vevidencead]         Destination:       [C:\User\yashwamthDesktop\vevidencedopsy.E0]
Source [C:Wsert/yashwamthDownloads/veridence#ler/wirdence#ler/wirdence#ler/wirdence#ler/wirdence#ler/wirdence#dopp=01
Destination: C\Users\yashwamth\Desktop\evidenceautopsy.E01
P
Progress Elevand Time 10:00 Time Bensining 10:00 Traveler Coard (MD/Car-) 0.0
Acquantum mogets
Event Log
Processing drive: C.V.Uservjavanumkth.Downkodk.twidencellet.veridence.adl         Image Fie Figure: Encase v & 10         Segment tize: 2000 HB         Case Name: 1         Urigate Descriptor: Autory Image         Urigate Descriptor: Autory Image         Image Field Hard: 10/18/2017 811:06 FM         Image Field Hard: 10/18/2017 811:06 FM         Expendent time: 0000         Source 0HALSHatt: das30seffectHeb032558/sef56011930.dd00709         Source 0HALSHatt: das30seffectHeb032558/sef56011930.dd00709         Source 0HALSHatt: das30seffectHeb032558/sef56011930.dd00709         Source 0HALSHatt: das30seffectHeb032558/sef56011930.dd00709
(2 Book France)

Figure 53: Image converted and summary.

# Summary

In this chapter, we have created the evidences for our investigation which can be done by creating an image file and analyzed using two different tools FTK toolkit and. We will create image files for the evidences passed into the Hard Drive Disk and Solid-State Drive in the next chapter. We use HD shredder for formatting the drives before getting them ready for the investigation.

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

# Introduction

In this chapter, we will go through the images creation of both HDD and SSD using FTK imager and converting them to E01 format using Forensic Imager for Analyzing the results in Autopsy. We will compare number of hits with the original files we passed and comparing the results of SSD with HDD. We will graphically analyze hits obtained during keyword searches in both tools.

#### Results

**Creating image of HDD**. While creating the Image of an HDD we use logical drive option instead of Physical drive as we are creating image of a specific drive that is externally connected to the system. We are suing an external device connected to investigation laptop.



Figure 54: HDD connected to Laptop 1.

8		Acces	sData FTK Imager 4.1	.1.1	- 🗇 🗙
<u>F</u> ile <u>V</u> iew <u>M</u> ode <u>H</u> elp					
🗛 🏩 🗣 🚓 🖛 🔂 🖬 🖬 🚑 🚑 👄 🚥	🖪 🥄   🗋 🗎 🗎 🐱	x x x			
Evidence Tree ×	File List				×
	Name	Size Type	Date Modified		
	1				
Custom Content Sources ×	1				^
Evidence:File System Path File Options					
< >					
New Edit Remove Remove All Create Image					
Properties Hex Value Inter Custom Conte					>
For User Guide, press F1					NUM

Figure 55: Home screen of FTK.

Ø		Access	Data FTK Imager 4.	1.1.1		_ 8 ×
<u>F</u> ile <u>V</u> iew <u>M</u> ode <u>H</u> elp						
🗛 🍕 🗞 🏟 🚰 🖬 🖬 🗛 🕳 🚥	🔁 ९   🗅 🖹 🖬 🐱 😸	h \Re 💡 🖕				
Evidence Tree ×	File List					
	Name	Size Type	Date Modified			
Custom Content Sources × Evidence:File System (Path (File Options		Please Select the Source Physical Drive Cogical Drive Contents of a Folde (opical file-level an Fernico Device (m.)	Select Source Evidence Type	rd, unaliocated, etc.)	×	^
Kew         Edit         Remove         Amove & game         Streate Image           Properties         Hex Value Inter         Custom Conte	r	< Back	Next > (	Cancel Help		~
For User Guide, press F1						NUM

Figure 56: Selecting option from type of device.

The hard Drive that we connected to laptop is shown as D drive, so we are selecting the option D drive from the list as shown in the figure below.

elect Drive				2
Source Drive	e Selection			
Please sel	lect from the folic Volume [NTFS]	owing available d	rives:	-
🗖 Autom	ate multiple remo	ovable media		
	< Back	Finish	Cancel	Help

Figure 57: Selecting HDD drive for image creation.

Evidence Item information is given in next step by giving Case Number, Examiner

name.

9		A	ccessData FTK Imager 4.1.1.1	- 0	l ×
<u>File View Mode H</u> elp					
1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	📴 🍾 🗋 🖻 🖻 🐱 🗃	<u>* 118</u> 7 .			
Evidence Tree ×	File List				
	Name	Size Type	Date Modified		
			Create Image		
			Evidence Item Information ×		
		Case Number:	defence		
		Evidence Number:	1		
		Unique Description:	ftkdefence		
		Examiner:	yash		
		Notes:			
Custom Content Sources ×					~
Evidence:File System Path File Options					
			Back Next > Cancel Help		
			Cancer		
< >					
New Edit Remove Remove All Greate Image					~
Properties Hex Value Inter Custom Conte					
For User Guide, press F1				N	UM

Figure 58: Create image evidence item information.

8	AccessData FTK Imager 4.1.1.1 – 🗖 🛛 🔺
<u>File View M</u> ode <u>H</u> elp	
🏫 🎎 🗣 🏫 🏤 🎦 🖬 🖬 🚓 🖂 🛏 🖿	📴 🔧 🗋 🗎 🐜 諸 🤹 🔹
Evidence Tree ×	File List
	Name Size Type Date Modified
	Create Image ×
	Select Image Destination
	Image Destination Folder
	C:\Users yeah:\Desktop Browse
	Image Filename (Excluding Extension)
	levednce
	For Flaw E11 and AEF formats D action of framework
Custom Content Sources X	Compression (0=None: 1=Fastest
Evidence:File System Path File Options	Use AD Encryption
	Filter by File Owner
	< Back Finish Cancel Help
	Sart Canal
< >	
New Edit Remove Remove All Greate Image	
Properties Hex Value Inter Custom Conte	
For User Guide, press F1	NUM

Figure 59: Selecting the destination for image of HDD.

9	AccessData FTK Imager 4.1.1.1	- 8 ×
<u>File View M</u> ode <u>H</u> elp		
요 않 \$ \$ 소 소 급 문 문 모 고 ㅋ	🔋 🌒 🔤 🖮 🧱 🦹 📜	
Evidence Tree ×	File List	
	Name Size Type Date Modified	
	Create Image X	
Custom Content Sources × Evidence:File SystemPath)File Options	Add     Edit     Remove       Add Overflow Location     Add Overflow Location       ✓     Verify images after they are created     Precalculate Progress Statistics       ✓     Create directory Istings of all files in the mage after they are created	Â
Properties Hex Value Inter Custom Conte		
For User Guide, press F1		NUM

Figure 60: Create image destination path.

Here we can select the image format by default the image is created as "DD" or "AD" format for FTK.

Cre	ate Image	$\times$
Sele	ect Image Type	$\times$
[	Please Select the Destination Image Type	
	Raw (dd)	
	O SMART	
	O E01	
	CAFF	
	< Back Next > Cancel Help	
	Start Cancel	

Figure 61: Selecting the type of image format.

9		A	ccessData FTK Imager 4.1.1.1	- ć	) × (
<u>File View M</u> ode <u>H</u> elp					
🟫 🏟 🗣 🚓 🚖 🔂 🖬 🗟 🚓 프 🚥	1 🖸 🔍 1 D 🗎 🗎 😽 🔒	1 🖹 🕺 🔋 🔒			
Evidence Tree ×	File List				×
	Name	Size Type	Date Modified		
			Create Image		
			Evidence Item Information ×		
		Case Number:	defence		
		Evidence Number:	1		
		Unique Description:	ftkdefence		
		Examiner:	yash		
	1	Notes:			
Custom Content Sources ×	1				~
Evidence:File System Path File Options					
			Back Next > Cancel Help		
			Start Cancel		
New Edit Remove Remove All Create Image					
Properties Hey Value Inter Curtom Conte	-				$\sim$
For User Guide, press F1	μ			Ν	UM

Figure 62: Unique identification for the image file.

The image size would be more or equal to the size of the drive. To fit the image into the device we fragment it into parts for easy analysis. We select fragmentation size from the below step. Here we are selecting 102400 MD size.

Create Image	$\times$
Select Image Destination	$\times$
Image Destination Folder	
D:\ Browse	
Image Filename (Excluding Extension)	
HDD Image	
Image Fragment Size (MB)       102400         For Raw, E01, and AFF formats: 0 = do not fragment       102400         Compression (0=None, 1=Fastest,, 9=Smallest)       0	
Use AD Encryption	
< Back Finish Cancel Help	
Start Cancel	

Figure 63: Selecting the fragmentation size for image of HDD (Marupudi, 2017).

The drive we are using to create image is 1TB external hard drive, so the image file may be equal to the size or of larger size, so we keep track of the time. Pre-Calculate progress is checked before starting the process.

Create Image			$\times$
Image Source			
Image Destination(s)	Starting Evidence Number:	1	
D:\HDD Image [raw/dd]			
Add	Edit Add Overflow Location	Remove	
<ul> <li>Verify images after they ar</li> <li>Create directory listings of</li> </ul>	e created  Precalculat all files in the image after the Start Cancel	e Progress Statistics y are created	

Figure 64: Verifying and starting the process of image creation of HDD.

Random pictures were captured during different stages of the image creation of the

HDD drive.

Creating Image [	0%] — — ×		Creating Image [3	34%] — 🗆 🗙
Image Source:	D:\		Image Source:	D:\
Destination:	D:\HDD Image		Destination:	D:\HDD Image
Status:	Creating image		Status:	Creating image
Progress Elaj Esti	229.25 of 953867.22 MB (19.104 MB/sec) psed time: 0:00:12 imated time left: 13:51:57	c	Progress Elap Estir	333540.75 of 953867.22 MB (11.368 MB/sec) sed time: 8:09:01 nated time left: 15:09:29
Creating Image (	Cancel	0	Creating Image [	
Image Source:	D:\	-	Image Source:	D:\
Destination:	D:\HDD Image	-	Destination:	D:\HDD Image
Status:	Creating image		Status:	Finished (WARNING: Bad sectorssee summary file)
Progress	1		Progress	
Elar Esti	621924.75 of 953867.22 MB (11.573 MB/sec) psed time: 14:55:38 mated time left: 7:58:01		Elap Esti	953867.22 of 953867.22 MB (9.501 MB/sec) osed time: 27:53:20 mated time left: 0:00:00
	Cancel		Image Summa	ry

Figure 65: Image creation of HDD at different intervals (Marupudi, 2017).

The images created from the drive are shown in the picture below it took more than one

day to create those files.

→   → I =   File Home Share	Drive Tools         New Volume (D:)           View         Manage	Becycle Bin		AccessData	
$\leftarrow \rightarrow \checkmark \uparrow \checkmark$ > This	PC > New Volume (D:)		GUI	FTK Imager	
Quick access     Desktop     Downloads	HDD Image HDD Image.001 HDD Image.001 HDD Image.002	Acrobat Reader DC	Oracle VM VirtualBox	HDShredder	
<ul> <li>Pictures</li> <li>iCloud Photo:</li> <li>iCloud Drive</li> </ul>	HDD Image.004 HDD Image.005 HDD Image.006 HDD Image.007	Dell SonicWAL	SAP Logon		
Junk Movies proposal	HDD Image.008	Google Chrome	Skype	HDD Image.010	Song

Figure 66: Image created of HDD (Marupudi, 2017).

Creating image of SSD. The same process is followed in creating an image of SSD.

Following are the screen shots captured for the same.

67



Figure 67: SSD connected to second laptop (Marupudi, 2017).

Select Source	$\times$
Please Select the Source Evidence Type         Physical Drive         Logical Drive         Image File         Contents of a Eolder (logical file-level analysis only; excludes deleted, unallocated, etc.)         Fernico Device (multiple CD/DVD)	
< Back Next > Cancel Help	

Figure 68: Selecting the logical drive for SSD image creation.

Select Drive	$\times$
Please select from the following available drives:           E:\ - New Volume [NTFS]	
Automate multiple removable media	
< Back Einish Cancel Help	>

Figure 69: Selecting SSD drive for image creation.

Create Image	$\times$
Select Image Type	$\times$
Please Select the Destination Image Type	
Raw (dd)	
C SMART	
C E01	
O AFF	
< Back Next > Cancel	Help
Start Cancel	

Figure 70: Selecting the destination for image of SSD.

Create Image		$\times$
Evidence Item Informati	on	$\times$
Case Number:	SSD 1	
Evidence Number:	SSD Evidence 1	]
Unique Description:	SSD Image	]
Examiner:	Shiva	1
Notes:	Image of SSD	]
	[]	
	< Back Next > Cancel Help	
	Start Cancel	

Figure 71: Selecting the type of SSD image.

Create Image	$\times$
Select Image Destination	$\times$
Image Destination Folder	
E:\ Browse	
Image Filename (Excluding Extension)	
Evidence Image	
Image Fragment Size (MB) For Raw, E01, and AFF formats: 0 = do not fragment	]
Compression (0=None, 1=Fastest,, 9=Smallest)	ł
Use AD Encryption	
< <u>B</u> ack <u>F</u> inish <u>C</u> ancel <u>H</u> elp	
Start Cancel	

Figure 72: Selecting the fragmentation size for image of SSD.

Image Source			_
\\.\PHYSICALDRIVE1			
	Starting Evidence Number:	1	
Image Destination(s)			
L. LVIGENCE IMage [raw/	aaj		
Add	Edit	Remove	
[]	Edit	Remove	
[Add]	Edit Add Overflow Location	Remove	
[Add]	Edit Add Overflow Location	Remove	
Lerify images after they	Add Overflow Location	Remove	

Figure 73: Verifying and starting the process of image creation of SSD.

incompany fill respect 1413			- 0 - 10			
a Yaw Mode Indu			Fig. Var. Mode mill			
			AND LO DUTAL	auste auffahren at 110 Mer 1.		
Annon Team - Mile List			Edentr Text	Patte		
Narw Site	Type Date Ma.			Name San Type Date We	4	
And Cafety Taxon	lige Textus,		Catar Gold Sawa Kelan In Somble. She Mark Somble. She Para Sawa Para Sawa Na Gang K		Internet PRII	- 0 ×
Die Xen Good Beb	and a submittee water.					
Evidence Tree	- File List					
97 Contractory (1997)	Narra Sire Type	Date Mrs				
Castorn Context Season Edition This Solves (Fall)	- Contrart	Greating Image Jinage Searce: Destination: Status: Program B D Tra	Supersonal constant Constant investor Constant investor Constant investor Territorial Constant investor Constant Consta			
K Barry (111) (111) (111)	> 					

Figure 74: Image creation of SSD at different intervals (Marupudi, 2017).

→ * ↑	> New	Volume (E:)			
Ouick access		Name ^	Date modified	Туре	Size
- Deskton		Evidence Image.001	6/15/2017 11:49 PM	001 File	104,857,600
Desciop	4	Evidence Image.002	6/16/2017 1:15 AM	002 File	104,857,600
Downloads		Evidence Image.003	6/16/2017 2:40 AM	003 File	104,857,600
Documents	Я	Evidence Image.004	6/16/2017 4:05 AM	004 File	104,857,600
Pictures	*	Evidence Image.005	6/16/2017 5:47 AM	005 File	72,131,584 K8
Defence2					
Defence4					
Music					
Videos					

Figure 75: Images created of SSD (Marupudi, 2017).

**Analyzing image of HDD in FTK**. After the image files are created for the HDD, the images are now analyzed using the FTK toolkit. The below image is the home page of the FTK after the image file is passed.

AccessData FTK 1.81.0 DE	MO VERSION				- 0
le Edit View Tools E	delp				
Overview Explo	Graphics	E-Mail	Search Bookmark		
Evidence Items	File Status	File			
Evidence Rems: 0	KFF Alert Files: 0	Documents			
File Items	Bookmarked Items: 0	Spreadshe	0		
Total File Items: 0	Bad Extension: 0	Databases	0		
Checked items: 0	Encrypted Files: 0	Graphics:	0		
Unchecked Items: 0	From E-mail: 0	Multimedia	0		
Flagged Thumbnails: 0	Deleted Files: 0	E-mail Mes			
Other Thumbnails: 0	From Recycle Bin: 0	Executable	essing Files		
Filtered In: 0	Duplicate Items: 0	Archives:	rent Evidence Item		
Filtered Out: 0	OLE Subitems: 0	Folders:	HDD Image 001		
Unfiltered Filtered	Flagged Ignore: 0	Slack/Free	ADD Illiage.001		
All Items Actual Files	KFF Ignorable: 0	Other Kno	rent File Item:		
	Data Carved Files: 0	Unknown	DD Image\New Volume-NTFS\HDD Image.001_08	0	7
M Evidence F Eviden	cc Path Display Name	e Identifi	Action Filtering Text Action Filtering Text Tile Type Urknown File Type Item Size: 26.214.400 (80 of 121) Progress: 26.050.560 at the case/system status every 10 0 minutes [	Elapsed Time: 0.00.13.45 Total Items Examined: 134 Total Items Added: 134 Total Items Added: 111 Log extended information Cancel	Comment
isted 0 Checker	1 Total 0 Highli	ighted			

Figure 76: Processing image 1 of HDD.

The keyword searches are done on the images processed to get the number of hits

obtained, below shows the hits of car.
		Income and the second s		Overview Explore	Graphics	E-Mail	Search	Bookmark	
le Status	File Category	"u ~ u" p	• 🐺 🖼 🕺 🔁 🔊	Indexed Search Live Search	ē	THE REAL PROPERTY AND INCOME.		7 Hits - [DriveFreeSpace2508] HDD Imagel/New Volume-NTFS\D     3 7 Hits - [DriveFreeSpace1423] HDD Imagel/New Volume-NTFS\D	riveFreeSpace2508 hiveFreeSpace1423
Files: 0	Documents: 4			La companya de la company	Canada Barrara		Not Colors	# 7 Hits - [DriveFreeSpace0338] HDD Image/New Volume-NTFS\D	riveFreeSpace0338
ed items: 0	Spreadsheets: 0			Indexed words Co	Jearchiteric		no ne	7 Hits - [DriveFreeSpace3593] HDD Image/New Volume-NTFS/D 7 Hits - [DriveFreeSpace3706] HDD Image/New Volume-NTFS/D	hiveFreeSpace3706
ision: 0	Databases: 0	and the second se	and the second se					7 Hits - [DriveFreeSpace2621] HDD Image/New Volume-NTFS\D	riveFreeSpace2621
i Files: 0	Graphics: 2							7 Hits - [DriveFreeSpace1650] HOD Image/New Volume-NTFS/D 7 Hits - [DriveFreeSpace1536] HDD Image/New Volume-NTFS/D	hiveFreeSpace1536
ait: 0	Multimedia: 0		and the second se		Toppare   Dermon	terri (Derrora 22)	Variat Barry Davis, Phys. 8	# 7 Hits - [DriveFreeSpace0565] HDD Image/New Volume-NTFS/D	riveFreeSpace0565
les: 173	E-mail Messages: 0				Cumulative operator.	NO OR View	Cumulative Results +	<ul> <li>7 Hits - [Driverreespaceus1] Hoo Image/New Yolume-NTPS/D</li> <li>7 Hits - [Car 1zt] HOO Image/New Yolume-NTPS/(orphan)/Car</li> </ul>	Car Lot
vole Bin: 0	Executables: 0			-				2.7. Hits 3DriveEneeSearce27351. HDD.Imanel.New.Volume.NTES.D	titueEreeSeace2735
tems: 29	Archives: 0	1. 10	100 m	People can form intimate	connections to their	cars in the cours	e of daily commute	es frustrating traffic iams, and liberating mad trips. How would you fe	el though if you
ems: 0	Folders: 14	1	CV.	insides, such as the reg	anity of your heartbe	eat and the amoun	t of glucose in you	ur blood?	
0.000 C	Slack Free Space AFE1		and the second states	Ford is experimenting wi	th all sorts of health a	and wellness featu	res for its cars and	d SUVs, according to Pim van der Jagt, a Ford R&D leader who desc	nbed some of the
able: 0	Other Knows Tune: 0	Southern Street Street	and the second second second	keynote talk at the IEEE	Body Sensor Netwo	rks Conference.			
aute. u	Other Known Type. 0	a construction of the second se	and the second se	"We've seen consumer s customers and give it an	pending on health an edge in the competit	id wellness going five automotive ma	up strongly," he lat	ter told IEEE Spectrum in an interview. That trend motivated Ford to v	work on health fea
ved haes: 0	Unknown Type: 329	and the second se		Chata a har a name a name a name		Poly of him a second		A Bada Constantin Condensaria	
OFF Unfibered	<ul><li>m</li></ul>	917		Photo: Nicole Randall	age at a contenence.	Dening nim a sci	een orsprays the te	ext boby Sensor Networks Conterence	
erri erriteres				<					
								VVdN	
	~ · >> 📥 🖽 🕅 🚱	D 🔊	Farm House 17.jpg					E-die Reers VVdN	
ETXcN			Zone Identifier				Cu	Zone.Identifier	
ETXcN			Farm House 18.ipg		~	~	n. vo	RCRD(	
Vaccine 10.jpj Vaccine 2.doc	7 ×		FILE0		FILEO	1		SI300	
Vaccine 2.jpg			Farm House 18.jpg		RCRD(	1P9		Application Form.pdr	15
Vaccine 3.jpg			RCRD(		Zone Iden	tifier		Deadth Certificate Form.pd	л
Vaccine 1.doc	×		Zone.Identifier		FILEO	10-10		Mortgage 1.jpg	
Vaccine 1.jpg			Farm House 19.jpg		RCRD(	1Pg		Mortgage 2.jpg	
IN TYPE IS					Zone Iden	tition.		Wortgage 3.10g	
ETACH			Frank Harris 40 inc		Inland 14	irora		INDV	

Figure 77: Files identified by searching keywords in image 1 of HDD.

We will analyze the results by identifying the number of files and number of hits by

individual keyword. Following is the results identified in Image 1 of HDD.

Overview 8	xplore	Graphics E-Mail	Se	arch		Over	view	Explore	Graphics	E-Mail	Sea	irch	
ndexed Search Live	Search					Indexe	d Search	Live Search					
Search Term:		Add	Import	Options	s	Searc	h Term:			Add	Import	Optio	ns
Indexed Words 0	.o	Search Items	Hits	Files	^	Inde	exed Words	s Co	Search Items		Hits	Files	1
		car	7132	1247					farm house		898	604	1
		dose	854	569					mortgage		145	579	
		islands	3981	573	~								•
		<		>					<			>	•
		Edit Item Remove Item Remove	All View Ite	m Results	5 >>				Edit Item Remov	Remove All	View Iter	n Resu	ts
		Cumulative operator: AND OR	View Cumulati	ve Results	S ≫				Cumulative operator:	AND OR Vie	w Cumulativ	e Resu	lts
				Te recount					ا م شد شد تحر ـ				

Figure 78: Results identified in image 1 of HDD.

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

shown below.

CHUU Image.	002		
urrent File Item			
IDD Image 2\	NONAME-Unknown\DriveFreeSpac	ce0148	
Current File Ite	m Status	Total Process Status	
Action:	Filtering Text	Elapsed Time:	0.00:05:04
File Type:	Drive Free Space	Total Items Examined:	148
	26,214,400 (148 of 4096)	Total Items Added:	148
Item Size:			

Figure 79: Processing image 2 of HDD.

Overview Explore	Graphics	E-Mail Se	arch		Overview	Explore	Graphics	E-Mail S	earch	
Indexed Search Live Search	1				Indexed Search	ive Search	1			
1		Add	Optio	ns	1			Add	Opti	ion
Indexed Words Co	Search Items	Hits	Files	^	Indexed Words	Co	Search Items	Hits	File	s
	car	6275	1153			· .	dose	753	502	
	Islands	3514	506				Mortgage	128.	. 506	
	dose	753	502	~			farm house	793.	. 508	
	<		)				<			>
	Edit Item Remove ite	Remove All View Ite	m Resul	ts »			Edit tem Remove iten	Remove All View 1	em Res	ul
	Internet and a second second	OP View Cumulati	ve Desu	Pe			Internet Contractory Contracto	OR View Cumula	tive Dee	

Figure 80: Results identified in image 2 of HDD.



Figure 81: Files identified by searching keywords in image 2 of HDD.

Ten image files obtained are analyzed by searching for the keywords in each image. The cumulative results of the hits obtained in HDD are shown below in the table.

Table 1

Keyword	Files in HDD	Hits in HDD
Car	1099	5731
Medicine	460	688
Phone	462	3208
Farm House	467	7272
Laptop	463	1201

Results Obtained from Images of HDD in FTK

Analyzing image of SSD in FTK. The same process of Image creation and analyzing

the images using FTK Toolkit is followed for SSD. Following are the steps followed.

E-Mail Search	Bookmark		THE LYNNER OF LEVE		
E-Mail Search     Add Evidence to Case     Any number of evidence ite     Acquired image of r     Local drive:     Folder:     Individual File:     The default refinements can all     folders. To make these furth     Add Evidence     Display Name	Bookmark  Add Evidence  so can be added to the case. There are several types of exist  itive: Several formatis supported, can be an image of a logic can be a logical or physical drive Adds at lifes in the specified folder, including contents. Adds a single file. NOTE: Disk image files should be a rs, set previously, can be oversidden independently for each be made. These enformemts can can be an include the exclusion of d or ref Add Evidence to Case  Type of Evidence to Add to Case  Add Evidence to Add to Case  Can be all Folder  Continue Cancel	ence tems: al or physical drive of subfolders ded as acquired images, evidence tem, and additional des/size ranges, awell as spec- hefme Evidence - Advanced. efme Evidence - Advanced. Time Zone Comment	Any number of evidence its Acquired image of Local drive: Folder Individual File: Individual File: Individual File: Individual File: Individual File: Individual File: Individual File: Display Name	Add Evidence ema can be added to the case. There are several types of evidence Evidence Information Evidence Information Evidence Information Evidence Information Evidence Information Comment Comment Code Evidence Time Zone Code Evidence Code E	Coll drive Sers soquired mages. s tem, and additional ranges, as well as use Evidence - Advanced idence - Advanced. 2 Zone Comment

Figure 82: Adding evidence to analyze results of SSD (Marupudi, 2017).

d Words Co	Search Items	Hits F	iles				
		Processing Files	-				
	Edit Rem   Remove Rem   Rem	Current Evidenc	e Item:				
		E:\Evidence Im	age.001				
	Cumulative operator. And OK	Current File Item				-	
- A. 1	**************	Evidence Imag	e\Part_1\NONAME-Unknown\Driv	veFreeSpace0002			
		Current File Ite	m Status	Total Process Status			
		Action	Filtering Text	Elapsed Time:	0.00.00.03		
n Luci de line		File Type:	Drive Free Space	Total Items Examined:	2		
8 1 for the 105		Item Size:	26,214,400 (2 of 83887)	Total Items Added	2		
	Full Path	Progress:	25,886,720	Total Items Indexed	1	Mod Date	Acc Da
		Log the case/sy	stem status every 10 葦 minute	s Log extended information	Cancel		

Figure 83: Processing image 1 of SSD (Marupudi, 2017).

Overview Explor	e Graphics E-I	fail Search	Bookmark				
Indexed Search Live Search	h						
Search Term:	Add	Import Option	\$				
Indexed Words Co	Search Items	Hits Files					
		Processing Files_					
	Edit Same Damara Barr	Current Evidence Item	é.				
	Cumulative operator: AND OR	E:\Evidence Image.0	02				
	Company operator. And OR	Current File Item					
n 🔳 🗸 n,	Evidence Image/NONAM			pace0004			
		Current File Item Sta	tus	Total Process Status			
		Action	Filtering Text	Elapsed Time:	0.00.00.04	Ī.	
	D 99	File Type:	Drive Free Space	Total Items Examined:	4		
9 8 88   48 🕌   16		Item Size:	26,214,400 (4 of 4096)	Total Items Added	4		
file Name	Full Path	Progress:	5,150,402	Total Items Indexed:	3	Mod Date	Acc Date
		Log the case/system	status every 10 🖨 minutes	Log extended information	Cancel		
					0		

Figure 84: Processing image 2 of SSD (Marupudi, 2017).

Search Term:	Add	Import C	Options					
Indexed Words Co	, Search Items	Hits F	iles					
		Processing Files.	-			1		
	Edit dem Remove lem Remo	Current Evidence	a Item:					
	Cumulative operator: AND OR	E:\Evidence Im-	age.003					
		Current File Item	S			-		
M.	₩₩₩₩₩₩₽ ₽0	Evidence Image	NONAME-Unknown\DriveFreeS	pace0003				
		Current File Iter	m Status	Total Process Status				
		Action	Filtering Text	Elapsed Time:	0.00.00.02	-		
File Type			Drive Free Space	Total Items Examined:	3	-		
		Item Size:	26,214,400 (3 of 4096)	Total Items Added	3	11.10.1	4	1.0
le Name	Full Path	Progress:	19,311,515	Total Items Indexed	2	Mod Date	Acc Date	L-Su
		Log the case/sy	stem status every 10 📮 minute	Log extended information	Cancel			

Figure 85: Processing image 3 of SSD (Marupudi, 2017).

Indexed Search							
Live Search	1	interesting and the	and a second sec				
Search Term	DDA	Import Op	ions				
Indexed Words Co	Search Items	Hits File					
		Processing Files_					
	Edition Description 10	Current Evidence II	em				
	Cumulative energianter	E:\Evidence Imag	e.004				
	Companye operator: AND OR	Current File Item				1	
n 🗖 🗸 🖓		Evidence ImageV	IONAME-Unknown\DriveFreeS	pace0004			
		Current File Item	Status	Total Process Status			
		Action	Indexing	Elapsed Time:	0.00:00:06	-	
a n na l <i>u</i> a 🌰 lina	D & or Unfiltered	File Type:	Drive Free Space	Total Items Examined:	4	-	
Elle Manne	E. I Dath	Item Size:	26,214,400 [4 of 4096]	Total Items Added:	4	Mad Date	Acc Date
nie Name S	run Path	Progress:	4%	Total Items Indexed:	4	mod Date	Acc Date
		Log the case/syste	m status every 10 🚭 minute	E Log extended information	Cancel		

Figure 86: Processing image 4 of SSD (Marupudi, 2017).

Current Evidence	Item:		
E:\Evidence Ima	age.005		
Current File Item:			
Evidence Image	NONAME-Unknown\DriveFreeS	pace0006	
Current File Iter	n Status	Total Process Status	
Action:	Filtering Text	Elapsed Time:	0.00:00:08
File Type:	Drive Free Space	Total Items Examined:	7
Item Size:	26,214,400 (7 of 2818)	Total Items Added:	7
Progress:	7,525,948	Total Items Indexed:	6

Figure 87: Processing image 5 of SSD (Marupudi, 2017).

Five image files that are obtained after imaging the SSD are analyzed and the

cumulative results obtained are shown in the below table.

Table 2

Results Obtained from Images of SSD in FTK

Keyword	Files in SSD	Hits in SSD
Car	760	1824
Medicine	144	215
Phone	30	245
Farm House	31	5633
Laptop	28	882

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

# Table 3

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

#### Comparing the Results Obtained in FTK

## Graphical representation of Hits in FTK.



Figure 88: Difference in results identified by number of files in FTK.



Figure 89: Difference in results identified by number of Hit in FTK.

**Analyzing Image of HDD in Autopsy**. The image files that are converted using the Forensic Imager is now analyzed using autopsy tool. The Image files which are in E01 format are now passed into a new case created in Autopsy using following steps and then a keyword search is done to analyze the number of hits in both the images created for HDD and SSD.

 New Case Information		×	
Steps  . Case Info  . Additional Information	Case Info  Enter New Case Information: Case Name: Base Directory: C:(JJsers/yashwamth/Desktop) Case Type: Single-user Case data will be stored in the following directory:	Browse	
	< Back Next > Finish Cance	Help	

First step involves creating a case and a database to analyze the case.

Figure 90: New case information.

Next step, we give required details for creating a case folder in local system by specifying base directory and case Name. We can also specify if the case is for a single user or a multiple user using the options.

ase View Tools Window Help					
Add Data Source 🕼 View Images/Vie	deos 🧱 Timeline 📗 Generate Rep	ort 🚺 Close Case		🔺 💿 🕶 Keyw	ord Lists 🔍 Keyword Search
	😹 New Case Information			×	
	Steps	Additional Inform	mation		
	1. Case Info 2. Additional Information	Optional: Se	et Case Number and Examiner		
		Case Number:	1		
		Examiner:	Yash		
	_				
			< Back Next > Finish	Cancel Help	

Figure 91: Set case number and examiner.

Next step, we provide details of the case number and the examiner details and click on

finish button to start creating a case folder and database.

ise View Tools Window Help			
🛉 Add Data Source 📠 View Images/Videos 🗱 Timeline 📗 Genera	te Report 🗾 Close Case	Keyword Lists	🔍 Keyword Search
	No. c. c.		
	Creating Case		
	Creating case database		
	Cancel		

Figure 92: Creating a case database.

Next Step, Index of the files are created for searching during analysis. This will help in faster keyword retrieval.

🕂 Add Data Source 📠 View Images/Nideos 🗱 Timeline 📓 Generate Report 🐻 Gose Case	Keyword Lists	Cr Keyword Search
Solr Keyword Search Service Opening Case Resources		

Figure 93: Creating new text index.

Next step, we will add the image file to the case space we created. Adding data source to

the case file.

ase View Tools Window Help			
🕂 Add Data Source 📠 View Ima	iges/Videos 🗮 Timeline 📗 Genera	ate Report 💊 Close Case 🔬 🔍 🐼 Keyword Lists	earch
	😹 Add Data Source	x	
	Steps	Select Type of Data Source To Add	
	Select Type of Data Source To Add     Select Data Source     Configure Ingest Modules     Add Data Source	Disk Image or VM File	
		Local Disk	
		Logical Files	
		Unallocated Space Image File	
		< Back Next > Finish Cancel Help	

Figure 94: Selecting type of data source.

Next step, we will browse the data source and select the converted image file which is in

E01 format.

K Fvidence - Autonsv 4.4.0		— П Х
Case View Tools Window Help		
Add Data Source 🜆 View Images/Videos 🗮 Timeline 📗 Genera	te Report 💊 Close Case 🔬 🕢 • Keyword Lists	Q- Keyword Search
Add Data Source		×
Steps	Select Data Source	
1. Select Type of Data Source To	Browse for an image file:	
Add 2. Select Data Source	C:\Users\yashwamth\Desktop\evidenceautopsy.E01 Browse	
3. Configure Ingest Modules 4. Add Data Source	Please select the input timezone: (GMT-6:00) America/Chicago $\scriptstyle \lor$	
	Ignore orphan files in FAT file systems	
	(faster results, although some data will not be searched)	
		_
	< Back Next > Finish Cancel Help	
		-

Figure 95: Browsing image file.

Next step, we will configure the ingest modules which will create a hash and makes

keyword search faster.

😹 Evidence - Autopsy 4.4.0				- 🗆 X
Case View Tools Window Help				
🕂 Add Data Source 📠 View Image	es/Videos 🗮 Timeline 📗 Generat	e Report 💊 Close Case	🔥 💿 🗸 Keyword Lists	Q- Keyword Search
	😹 Add Data Source		×	
	Steps	Configure Ingest Modules		
	Select Type of Data Source To Add     Select Data Source     Configure Ingest Modules     Add Data Source	Run ingest modules on: All Files, Directories, and Unallocated Space	The selected module has no per-run settings.	
		Reactification      Reactification      File Type Identification      Embedded File Extractor      Exif Parser      Keyword Search      Email Parser      Extension Mismatch Detector      Extension Mismatch Detector      Interesting Files Identifier      PhotoRec Carver      Virtual Machine Extractor      Android Analyzer		
-		Select All Deselect All History	Extracts recent user activity, such as Web browsing, recenti Global Settings	
			< Back Next > Finish Cancel Help	

Figure 96: Configure ingest modules.

The keyword search is made using the five keywords and the below results are obtained from the hits in both SSD and HDD.

# Table 4

Results Obtained from Images of HDD in Autopsy

Keyword	Files in HDD	Hits in HDD
Car	1167	6576
Medicine	479	645
Phone	454	3109
Farm House	475	7348
Laptop	498	1389

# Analyzing Image of SDD in Autopsy.

## Table 5

# Results Obtained from Images of SSD in Autopsy

Keyword	Files in SSD	Hits in SSD
Car	765	1678
Medicine	144	215
Phone	32	245
Farm House	35	5788
Laptop	31	864

## Table 6

Comparing the Results Obtained in Autopsy

		Files	Files		Hits	Hits
	Original	in	in	Original	in	in
Keyword	Files	HDD	SSD	Hits	HDD	SSD
Car	1964	1167	765	9181	6576	1678
Medicine	764	479	144	1045	645	215
Phone	555	454	32	5532	3109	245
Farm House	692	475	35	14954	7348	5788
Laptop	1161	498	31	3588	1389	864

**Graphical representation of hits in Autopsy**. Visualizing number of files obtained from HDD and SSD in Autopsy through Chart.



Figure 97: Difference in results identified by number of files in autopsy.

Visualizing number of files obtained from HDD and SSD with original files passed in



Autopsy through Chart.

Figure 98: Difference in results identified by number of Hit in autopsy.

## Conclusion

Same Evidence file is created for both the storage devices SSD and HDD which are formatted using the HD Shredder to wipe out data completely, passed with different combinations of data that has been taken as an evidence which are being transferred. FTK Imager is used to create the image files of the drives (SSD and HDD) to analyze then using an investigator's laptop which has FTK Toolkit and Autopsy tool in it. However, due to the functionality of the devices and other factors that we discussed in the paper it is evident that the results of the evidences are different in both drives.

In this paper, we have discussed about the features of Solid State Drives, their advantages and mechanism of storage as well as other important features. Based on the study we conducted, and the results obtained from the experiment using FTK and Autopsy it is proven that SSD's has a phenomenon to destroy or loss critical evidences which may create trouble for the forensic investigators with the existing tools for finding key evidence and resolving cases that were solved by using traditional methods on HDD.

#### References

- Aaronson, L. (2008). *How it works: The sturdiest solid-state storage*. Retrieved April 15, 2017, from http://www.popsci.com/node/19967.
- AccessData. (2017). *AccessData*. Retrieved from http://accessdata.com: http://accessdata.com/solutions/digital-forensics/forensic-toolkit-ftk.
- Amazon.ca. (2017). *Solid state drives*. Retrieved from https://www.amazon.com/Samsung-2-5-Inch-Internal-MZ-75E4T0B-AM/dp/B01G844OOO.
- Amazon.ca (2017). *Internal structure*. Retrieved from https://www.amazon.com/Samsung-500GB-mSATA3-Solid-Retail/dp/B00HWHVOQS.
- Azemovic, J. (2010, August 27). *SQL Server Pro*. Retrieved from http://sqlmag.com/sql-server/csi-sql-server.
- Chen, F., Koufaty, D., & Zhang, X. (2016). Hystor: Making the best use of solid state drives in high performance storage systems. In Conference Proceedings of the 25<sup>th</sup> International Conference on Supercomputing, Tucson, AZ, May 31-June 4.
- Computer Hope. (2017a). *Advantages of SSD over HDD*. Retrieved from http://www.computerhope.com/issues/ch001396.htm.
- Computer Hope. (2017b, October 17). *HardDrive*. Retrieved from https://www.computerhope.com/jargon/h/harddriv.htm.

Dennon, A. (2016, January 29). *The digital forensics process*. Retrieved from PICPA: https://www.picpa.org/articles/cpa-now-blog/cpa-now/2016/01/29/the-digital-forensicsprocess. Edwards, B. (2012, January 17). *http://www.pcworld.com*. Retrieved from pcworld: http://www.pcworld.com/article/246617/storage/evolution-of-the-solid-state-drive.html.

- Encase. (2017). *Software guidence*. Retrieved from www.guidancesoftware.com: https://www.guidancesoftware.com/encase-forensic.
- ESSD Embedded. (2017). *Embedded SSD*. Retrieved from https://product.tdk.com/info/en/ techlibrary/archives/techjournal/vol15\_essd/contents03.html.
- Evan Amos. (2017, October). *Wikipedia*. Retrieved from https://en.wikipedia.org/wiki/ Hard\_disk\_drive#/media/File:Laptop-hard-drive-exposed.jpg.
- Evans, C. (2012, August). *Flash! All-solid-state arrays*. Retrieved April 15, 2017, from http://searchstorage.techtarget.com/ magazineContent/Flash-All-solid-state-arrays.
- Fisher, T. (2017, September 12). *LifeWire*. Retrieved from https://www.lifewire.com/what-is-a-hard-disk-drive-2618152.
- Garfinkel, S. L. (2013, October). *Modern crime often leaves an electronic trail. Finding and preserving that evidence requires careful methods as well as technical skill*. Retrieved from http://www.americanscientist.org: http://www.americanscientist.org/issues/ pub/digital-forensics.
- Harris, W. (2015). *How stuff works*. Retrieved from http://computer.howstuffworks.com: http://computer.howstuffworks.com/solid-state-drive.htm.
- Humphries, M. (2017). *Geek*. Retrieved from http://www.geek.com: http://www.geek.com/ chips/toshiba-hard-drives-will-be-40tb-by-2020-ssds-will-be-128tb-by-2018-1632425/.

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

Janorkar, P. (2015, August 19). Seminar topics.

Kerekes, Z. (2017). *Storagesearch*. Retrieved from http://www.storagesearch.com: http://www.storagesearch.com/chartingtheriseofssds.html.

- LifeWire. (2017, September). *LifeWire*. Retrieved from https://www.lifewire.com/how-to-wipe-a-hard-drive-2624527.
- Marupudi, S. S. (2017). Solid state drives: New challenge for forensic investigation. *Solid State Drives: New Challenge for Forensic Investigation*.
- Masuoka, F. (1987). New ultra high density EPROM and flash EEPROM with NAND structure cell. *IEEE*, Electron Devices Meeting, 1987 International. IEEE. Retrieved 04-15-2017.
- Mellor, C. (2013, May 9). *The register*. Retrieved from https://www.theregister.co.uk/2013/ 05/09/ihs\_on\_pc\_hdd\_ssd\_units/.
- Mizota, K. (2015, 01 07). *Encase-forensic*. Retrieved from http://encase-forensicblog.guidancesoftware.com/search/label/Decryption.
- Newegg. (2017). *Newegg*. Retrieved from https://www.newegg.com/Product/Product. aspx?Item=N82E16820147467.
- Ngo, D. (2012, August 22). *Storage talk: Why you should get an SSD and keep your HDD, too.* Retrieved April 15, 2017, from https://www.cnet.com/news/storage-talk-why-you-should-get-an-ssd-and-keep-your-hdd-too/.

- Ngo., D. (2013, March 1). *Digital storage basics, Part 4: SSD explained*. Retrieved April 15, 2017, from CNet: https://www.cnet.com/how-to/digital-storage-basics-part-4-ssd-explained/.
- Rouse, M. (2016, May). *Searchsolidstatestoragetechtarget*. Retrieved from TechTarget: http://searchsolidstatestorage.techtarget.com/definition/SSD-solid-state-drive.
- S.A.S., A. (2017). *DFF homepage*. Retrieved from digital-forensic: http://www.digital-forensic.org/.
- Seagate. (2012, August 22). *The top 20 things to know about SSD*. Retrieved April 15, 2017, from Seagate: http://www.seagate.com/files/docs/pdf/ssd-faq-us.pdf.
- Shankdhar, P. (2017). *InfosecInstitute*. Retrieved from http://resources.infosecinstitute.com: http://resources.infosecinstitute.com/computer-forensics-tools/#gref.
- Tools, K. (2014, May 16). Kali tools.
- wiki. (2017). Wikipedia. Retrieved from https://en.wikipedia.org/wiki/Forensic\_Toolkit.
- X-Ways. (2017). *Forensics*. Retrieved from www.x-ways.net: http://www.x-ways.net/forensics/.

X-ways. (2017). X-ways. Retrieved from http://www.x-ways.net/pics/xwf\_screen\_eng.png.