5-2020

Comparing SSD Forensics with HDD Forensics

Varun Reddy Kondam
varun.reddy0796@outlook.com

Comparing SSD Forensics with HDD Forensics

By

Varun Reddy Kondam

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 2020

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

Abstract

The technological industry is growing at an unprecedented rate; to adequately evaluate this shift in the fast-paced industry, one would first need to deliberate on the differences between the Hard Disk Drive (HDD) and Solid-State Drive (SSD). HDD is a hard disk drive that was conventionally used to store data, whereas SSD is a more modern and compact substitute; SSDs comprises of flash memory technology, which is the modern-day method of storing data. Though the inception of data storage began with HDD, they proved to be less accessible and stored less data as compared to the present-day SSDs, which can easily store up to 1 Terabyte in a minuscule chip-size frame. Hence, SSDs are more convenient and user-friendly, where, in contrast, HDDs often require some degree of technical knowledge. However, since SSDs are still a relatively new phenomenon, it has proved to create myriads of problems in the digital forensics department. Since SSDs are still a more modern concept, the tools that digital forensics employ to investigate evidence obtained from HDDs are not proving to be as efficient; this is primarily due to the fact that data in flash memory drives can only be written if the data unit or data block is erased, ergo, an erase operation occurs every time before something is written into the flash memory. Therefore, the aim of this research is to critically analyze the results obtained by running forensic tools on an HDD and SSD; the results would pertain to the image generated from the HDD and SSD.

Table of Contents

Page

List of Tables

Table Page

List of Figures

Figure Page

Chapter I: Introduction

Introduction

“Wherever the future computer technology may take us, at least we know that SSD will take us there quickly.” (Anonymous).

This chapter gives a brief introduction to Solid State Drives, Hard Disk Drives, and Digital forensics. Starting with Solid-state drives, generally termed as SSDs are storage devices that fall under the category of non-volatile memory storage devices. Nowadays, SSD is considered to be the primary/central data storage system. When it comes to size, SSDs are smaller, portable, and faster when storing data, fetching data, highly efficient, and very less consumption of power. Though it doesn’t have any physical disks to read/write data, it is also called as Solid-State Disk. SATA and SAS are two protocols, which are used by both Hard Disk Drive (HDD) and Solid-state drive (SSD). SSD uses a Flash memory technology, and NVM Express is the new I/O protocol developed to handle the requirements of Flash memory technology, which is used in SSDs, unlike HDDs (Ayusharma0698, 2018).

The conventional Hard Disk Drives, floppy disks are electromechanical drives, and they contain spinning disks, movable heads to read and write data to the drive. There are no moving parts or mechanical components in SSD (Ayusharma0698, 2018). SSDs can work twice as fast as the HDD, and this makes disk performance speed as the main advantage. The accurate speed of an SSD cannot be determined, because it usually depends on what all a person is doing on a computer at a time. Even if data is written to and from disk on a constant basis, that means if someone open applications, browse the internet, listen to music, play games or load a video, it was observed that everything goes smoother and faster if SSD is installed (Nield, 2018). Some of the basic differences like SSD has lower latency, whereas HDD has higher and SSD is more reliable compared to HDDs, more chances of mechanical components failure in HDDs makes SSD a highly dependent storage device these days. RAM is known as volatile memory/temporary memory because, when the system is turned off, memory stored in RAM is lost. SSD stores data even if the system/computer is turned off, and that makes it a non-volatile memory. After discussing the positive and negative aspects of SSD and HDD, this paper discusses the architectures of SSD.

Solid-state drives are designed and developed into two types based on their mechanisms: NOR flash and NAND flash. Right now, the second most popular flash architecture is the NOR architecture, which is commonly used in EPROM (Erasable Programmable Read-Only Memory) and EEPROM (Electrically Erasable Programmable Read-Only Memory) designs. This architecture needs one contact for two cells; these cells are arranged in parallel. This parallel arrangement makes it consume more space for configuration. To reduce this occupancy space for configuration, NAND architecture was developed. In this, the cells are arranged in series combination. Though this occupies less configuration space, this has a drawback of slow data reading compared to NOR (Flash memory NAND NOR, n.d.).

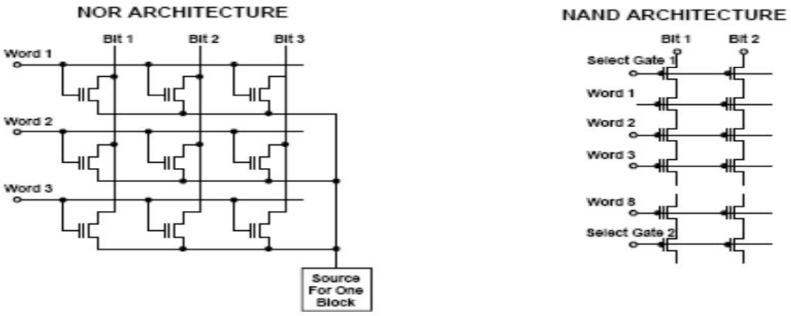


Figure 1: Architecture comparison *(Flash memory NAND NOR, n.d.)*

When it comes to the performance of these two architectures NAND and NOR, NOR reads data a bit faster than NAND, and NAND writes data faster than NOR. Usually, Data in flash memory can only be written if the data unit or data block is completely erased/empty. So, erase operation occurs every time before something is written into the flash memory. When it comes to memory capacity, NAND flash architecture memory capacity ranges from 1Gigabyte to 64Gigabytes, making this more capacity and less expensive. NOR flash architecture memory capacity ranges from 1Megabyte to 64 Megabytes, making this less capacity and more expensive. So far, it was just SSD; it's architecture and HDD. In the next topic, this paper introduces digital forensics.

Let it be an Organization, let it be an institution or let it be a house, each and every place has a computer and many other digital devices. It was unbelievable that computers or digital devices would be a part of criminal investigations, and since the 1970s, computers involving in crimes has increased rapidly. Then comes the Digital Forensics in the 1980s, playing a major role in the investigation. Slowly Digital Forensics gained its popularity and support. People involving in crime use some sort of digital devices like computers, laptops, mobile phones, etc. This helps digital forensic investigators to track the individual's actions involving in a crime scene. Digital forensics can be stated as a forensic science encompassing the recovery and material found in digital devices (Morton, 2015). Forensic investigators use different tools working on the respective memory storage drives. This paper discusses some of the Digital forensic tools working on both SSD and HDD, comparing their results and challenges faced during this forensic investigation.

Problem Statement

In the past few years, no one would have imagined how much technology has developed. It was so surprising when most of the evidence involving in crime are recovered from digital devices. Forensic investigation on digital devices plays a key role in crime investigations. The storage mechanisms of different devices are varying day-by-day as the technology is booming. This makes forensic investigator's job difficult. This research paper problem statement is to pick different forensic tools, work on both SSD and HDD drives by extracting images before and after deleting the evidence files and understand/investigate the results obtained.

The objective of the Study

The main objective of the study is to understand the challenges faced by digital forensic investigators, finding deleted evidence files in SSDs, HDDs, by working on them using different forensic tools. This research includes the comparisons of results obtained from the SSD and HDD drives.

Study Questions

The study questions on this research include everything that’s basically related to the digital forensic investigation. What is a Digital Forensic investigation? How is a digital forensic investigation conducted/carried? What are different digital forensic tools and their purpose? What do you conclude from the results obtained?

Definition of Terms

Digital forensics Digital forensics commonly known as computer forensics is, presenting the study of any digital evidence found on digital media storage devices or computers by identifying, preserving, recovering, and analyzing the evidence (Stephens, 2016).

Digital evidence “Any data stored or transmitted using a computer that supports or disproves a theory of how an offense occurred of that address, critical elements of the offense such as internet of alibi” (Casey, 2011). Digital evidence is any kind of digital data that can link a crime to a victim or a suspect or prove the occurrence of a crime. This data comprises texts, pictures, video, and audio. Some examples of digital evidence are IRC (Internet Relay Chat) chat history, images, email archives, video surveillance, or log files that show access to certain resources (Geier, 2015).

Hard Disk Drive Hard Disk Drive is commonly known as a hard drive. This is a conventional type of data storage media. It has mechanical moving parts to read and write data to the disk platters (coated in magnetic media (Platter, 2017)). Hard disks in olden days can store megabytes of data, which is now increased to terabyte range.

Solid State Drive Solid state drive is commonly known as Solid State Disk. This is a non-volatile memory storage device. This does not have any mechanical moving parts, unlike HDD. Data is stored using flash memory instead of magnetic platters. These SSDs are more reliable and have zero latency (no moving head to read/write data (Definition of Encyclopedia, n.d)).

Flash memory This is a kind of Electrically Erasable Programmable Read-Only Memory (EEPROM). This can also be called as flash storage, and this is a type of non-volatile memory (Rouse, 2017). Data can be written only on erased blocks. This technology can be used in consumer devices like digital cameras, USB flash drives, tablet computers, mobile phones, etc.

Summary

In this chapter, a basic introduction to SSD and its functionality is discussed. The common functionalities in SSD and HDD are briefly explained. SSD is configured into two types based on its architecture: NAND and NOR. These two type's architecture diagrams and basic functionalities have been discussed. This chapter also discussed the importance of digital forensics in the past and present days with respect to the growing, updating technology. This research paper conducts a study in analyzing the results obtained from both SSD and HDD drives after running different forensic tools on them. The next chapter will discuss more on the background and literature review, one should be aware of before working on different forensic tools.

Chapter II. Background and Review of Literature

Introduction

This chapter is to know information regarding questions like how Digital forensics came into the picture, when and where it was started. Day-by-day many new forensic tools are being developed, and this chapter discusses some of such forensic tools and their purpose. This chapter will discuss more about Digital forensics, SSD, and HDD drive's behavior in response to the forensic tools. This chapter will also discuss the previous researches done or related to this problem.

Background and Literature Review

Forensics or Forensic science

Forensics is derived from Latin word *forensic*, which means debate or a public discussion. “Any science used for the purposes of the law is forensic science.” (What is Forensic science?, n.d.). Around the world, forensic science is used to solve civil conflicts by following government rules and implementing criminal laws to protect the victims or the public. In the mid to late 1800s, science was used to investigate crimes and identify criminals (Grossi, n.d.). In order to prove guilt or innocence between crime and suspect, evidence should be collected. This evidence acts as a link between a crime and a suspect.

Forensic science can be used to (Grossi, n.d.):

- Prove the elements of a crime

- Validate or question victim or suspect statements
- Recognize decedents or suspects
- Create a connection to a crime or crime scene

Three concepts are important to provide reliable evidence; they are Chain of Custody, Admissibility of Tests, Evidence and Testimony, Expert witness (Geier, 2015).

Whatever be the type of evidence, its documentation and evaluation are described in the chain of custody. Based on their nature, evidence like blood spatters, human corps cannot be preserved as they are. An investigator needs to be more cautious and careful while collecting such evidence during analysis, or else evidence may be destroyed easily. The evidence should be documented, evaluated, and imaged properly. These documents should be clear so that investigators can re-evaluate evidence any day, any time in the future. The location where the evidence is stored from the day it is documented to the present date should be clearly mentioned. Every change in location should be documented (Geier, 2015). If the documentation has a missing location or time, then the evidence will be rejected and cannot be provided in the court.

Admissibility of Tests, Evidence, and Testimony includes the existence of legal standards for the acceptance of forensic tests and testimony (Geier, 2015). From all the forensic science disciplines, the expert witness concept is considered as the third issue. A witness is a person who explains what he/she observed. An expert witness is an expert with discipline and will be able to give suggestions and opinions related to discipline. The witness need not be qualified or officially recognized, but an expert witness should be qualified and officially recognized by involving a legal authority.

These three concepts above mentioned are common for all different types of forensic science. Different types of forensic science are Forensic Toxicology, Forensic Dentistry, Forensic Medicine, and Digital Forensics, etc. (What exactly is Forensics?, n.d).

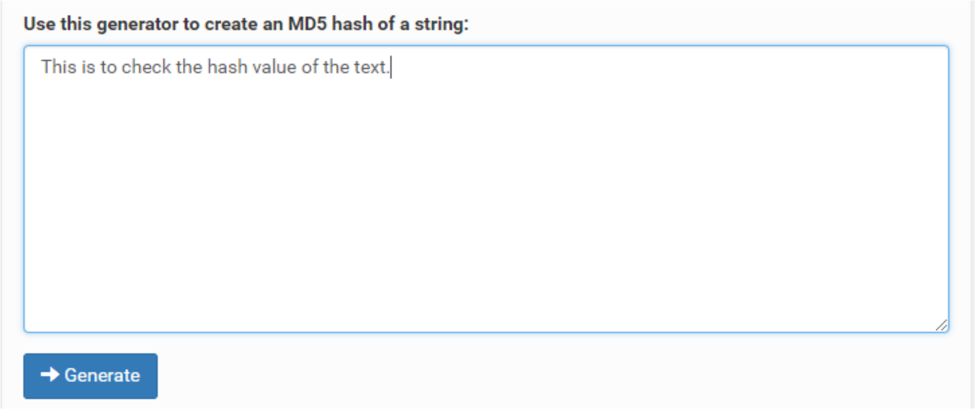
Digital forensics

Evidence can be found in digital on a suspect's digital devices or on the internet when a cr ime has been committed in the physical world many times. The internet has been expanding with more sensors monitoring the real world on a daily basis, such as ATM cameras, traffic cameras, webcams, and surveillance cameras. Usually, many people keep posting many messages on social media websites or chat through Internet Relay Chat (IRC) rooms, by which their IP addresses disclose their location and conversations that are being recorded. A digital forensic investigation must be conducted when an investigation is continuing, and there is a possibility of securing digital evidence. This digital forensic investigation basically comprises seizing and searching for possible evidence or leads on a suspect's digital devices such as personal computers, mobile phones, navigation devices, memory devices (Geier, 2015).

Digital forensics was commonly called ‘computer forensics’ until the late 1990s. The first persons to work on computer forensic were computer hobbyist law enforcement officers. Their work began in 1984, USA, in the FBI Computer Analysis and Response Team (CART). A year later, the Fraud Squad, a computer crime unit, was set up by John Austen (Metropolitan Police) in the UK. At the beginning of the 1990s, a major change took place. So many technical support operatives and crime investigators inside the UK law enforcement agencies and some other specialists realized that digital forensics requires protocols, procedures, and standard techniques. They decided to develop the formalisms. In 1994 and 1995, continuous conferences were conducted by Fraud Squad and the Inland Revenue at the Police Staff College in Bramshill, which led to the establishment of modern British digital forensic methodology (Price, n.d.). In the UK, the first version of the *Good Practice Guide for Digital Evidence* was developed in 1988 by the Association of Chief Police Officers (ACPO).

For example, T.J. Maxx, Marshalls and other retail stores parented by the company TJX in US, Canada, and Europe became the main target to the cybercriminals who stole 90 million credit and debit card numbers. These cybercriminals gained unauthorized access to the main channel of the TJX network in 2005. It took two years of observation for the cyberthieves to gather credit card numbers, debit card numbers, driver's license information, and social security numbers of all those customers, thus resulting in charge of $170 Million to TJX by the lawsuits (Geier, 2015). In 2009, Maksym Yastremskiy, a Ukrainian man, was arrested and sentenced to 30 years in prison for trafficking in credit card numbers stolen from TJX. The computers used by Yastremskiy had evidence, and this evidence was obtained with difficulties by the investigators. Later, in 2010 Albert Gonzalez entered the TJX network without authorization, stole their information, and was sentenced 20 years in prison (Prahlow, 2010).

When forensic professionals analyze a digital medium, the evidence must, therefore, be retrieved from deleted or lost data, broken or purposely destroyed memory. Irrespective of the device's state and the data, the first most important step to be taken is: investigator should create an image that is a digital copy of the device collected, in the same state as it was collected. This digital copy image is very important to prove the integrity of the evidence possibly found during the investigation, the chain of custody, so it can be proved that the data on the medium was not changed or altered by the investigator or any third party from the time the device was collected to the date it is presented in the court (Geier, 2015). Verifying the integrity of the evidence is a process in which the hash values are obtained and compared. A hash value is then computed checksum of the data. The digital evidence most probably has the hash value of the image. MD5 or SHA-1 are the two algorithms most commonly used for hash value generation. The output from the MD5 hash algorithm would be of size 128-bit. A small change in the file or image will generate a different hash value. This helps us in identifying if the evidence is altered or not. Let us understand this by a small example. In the Figure below, text entered is "*This is to check the hash value of the text.*" and generated the hash value using the MD5 algorithm.

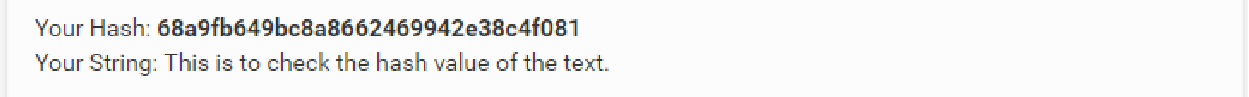


Use this generator to create an MD5 hash of a string:

This is to check the hash value of the text.

Figure 2: Text to generate the hash value *(MD5hashgenerator, n.d.)*

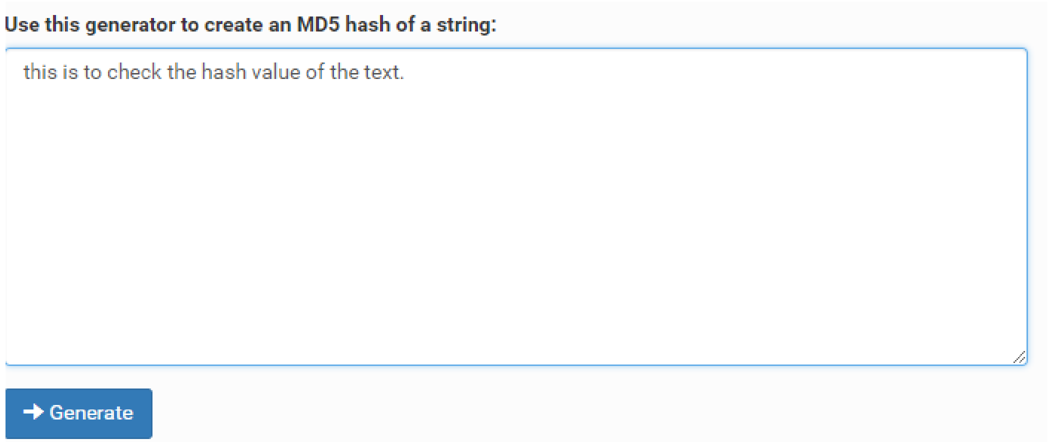
The figure below shows the hash value generated from the above text, i.e. "**68a9fb649bc8a8662469942e38c4f081**".



Your Hash: **68a9fb649bc8a8662469942e38c4f081**
Your String: This is to check the hash value of the text.

Figure 3: After generating a hash value

Now, change the first letter of the first word from the above text, uppercase to lowercase, i.e., “*this is to check the hash value of the text.*” The figure below displays text before generating the hash value.

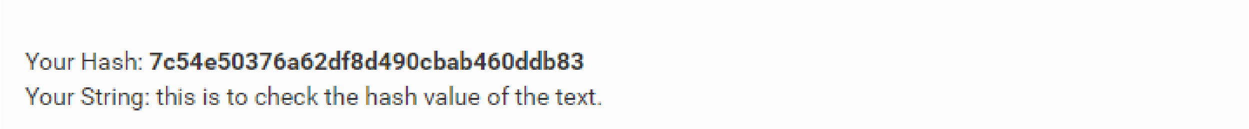


Use this generator to create an MD5 hash of a string:

this is to check the hash value of the text.

Figure 4: Altered text to generate a new hash value.

After generating the hash value, output is: **“7c54e50376a62df8d490cbab460ddb83”.**



Your Hash: **7c54e50376a62df8d490cbab460ddb83**
Your String: this is to check the hash value of the text.

Figure 5: The new hash value generated using MD5.

This can conclude that, even if there is a very small change or a single character change in the evidence, the hash value generated will be different. This makes it clearer that evidence has been altered and cannot be provided in the court law.

Table 1:

Different MD5 hash values for two texts.

Digital Message/Text	*MD5 Output*
This is to check the hash value of the text.	**68a9fb649bc8a8662469942e38c4f081**
this is to check the hash value of the text.	**7c54e50376a62df8d490cbab460ddb83**

This table compares the two different hash values generated for two different texts by the MD5 algorithm.

Digital Forensic Process

There should be a proper approach and understanding before a person deals with anything in this world, which is the reason why, for everything done, an outcome is expected and has a process of steps. For example, if someone wants to plant a garden, they can’t just dig a hole, throw seeds, and hope for the best. They need to follow a process involving steps to get a good result or outcome. Like this, there are four Digital forensic process steps to be followed by a digital forensic investigator/specialist. The number of steps is not limited to four or five; it keeps on changing depending on the environment the forensic specialists are investigating or working on. These four steps by NIST (National Institute of Standards and Technology) are Collection, Examination, Analysis, and Reporting.

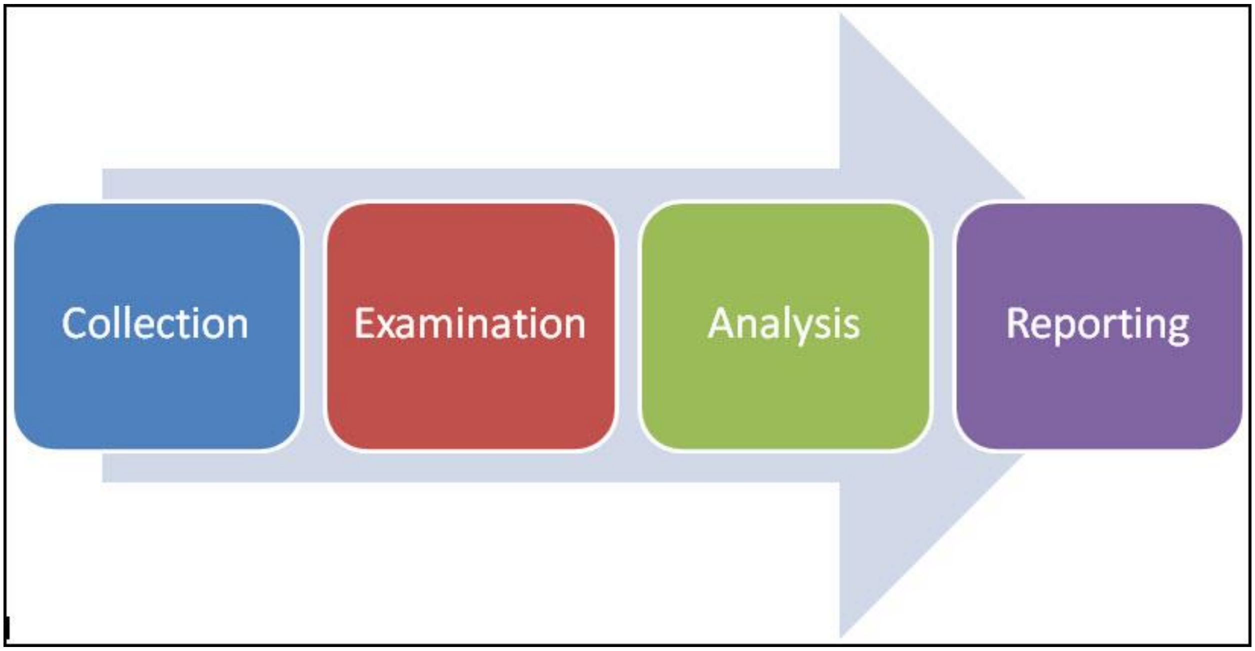


Figure 6: Digital forensic process steps *(Harrell, 2010)*.

Collection: This is considered as the first most important step in the digital forensic process. In this phase, the items that can be considered as evidence will be identified and collected (Valli, 2009). Before any process is started, the examiners should make sure that all the hardware and software are working. Every forensic organization should continuously check if their tools are working efficiently. They should retest it before and after any type of updates are being done (Carroll, Brannon, & Song, 2017). The digital media involving in the case will be collected and seized securely. A duplicate copy of the digital evidence will be created at the very first moment after the collection of evidence.

Examination: In this phase, after the digital media is collected, data needs to be extracted. A copy of whatever data or evidence found will be created. This copy is called an "image" (Computer Forensic Examination Steps. , n.d.). This process of image creation can also be called as data acquisition. A proper plan will be developed by the examiner before actually acquiring the data. Once the data acquisition is planned, and image files are created, the examiner verifies the integrity of evidence data. This can be verified by generating the hash values of the original evidence and an image copy of the evidence. Any search or examination should be done on image copies created. It is the responsibility of the examiners or investigators to make sure the original evidence is not altered. Data will be extracted or acquired without changing or damaging the source/original evidence. Examination or acquisition process step can simply be listed into three steps:

I. Develop a plan to acquire the data from evidence.
II. Acquire the data.
III. Verify the integrity of the data acquired.

After the evidence, data integrity is checked, and no changes are seen, then comes the analysis phase.

Analysis: In this phase, the evidence is extracted by understanding the collected information. Well organized standards and methodologies should be followed by the investigator during this procedure. The investigator can use other tools to perform additional actions, and this helps him/her obtain additional details, like deleted files. As noted above, these tools must be validated to ensure accuracy and reliability. The investigator extracts evidence from within the data collected by referring to the petitioner's documentation. Generally, there are two strategies: the investigator searches for something he doesn't know, within something he knows (Fahey, n.d.). This search includes programs that are infected, programs that are opened, documents erased, history of the internet browser, chat, and call history. The second thing, the investigator might be searching for something he knows in something he doesn’t know, i.e., understanding the unstructured data to extract valuable information like email addresses, URLs. Sometimes, this analysis helps in identifying the attacker’s location, attacker identity, and the scenario of the attack. An analysis result list will be created by the investigators. This includes all the results obtained from their analysis.

Reporting: Finally, all the investigators involving in a case repeat the above steps enough times and generate a forensic report (Carroll, Brannon, & Song, 2017). All the steps performed during the investigation will be clearly listed with a detailed description in the report. This description includes the personal details, who has done the examination, what kind of software/hardware tools were used during this investigation, photographs if any were taken, obtained hash values, etc. This also includes media details like hard disks, computer memory files, log entry, etc. Therefore, this final forensic report is very important because this tells us the whole process involved in an investigation (Palmer, 2001).

An enhanced digital forensic model known as Abstract Digital Forensic Model (ADFM) was later proposed by authors Reith, Carr & Gunsch (Mark Reith Clint, 2002). This model has an extra number of phases, making it clearer for digital forensic investigators.

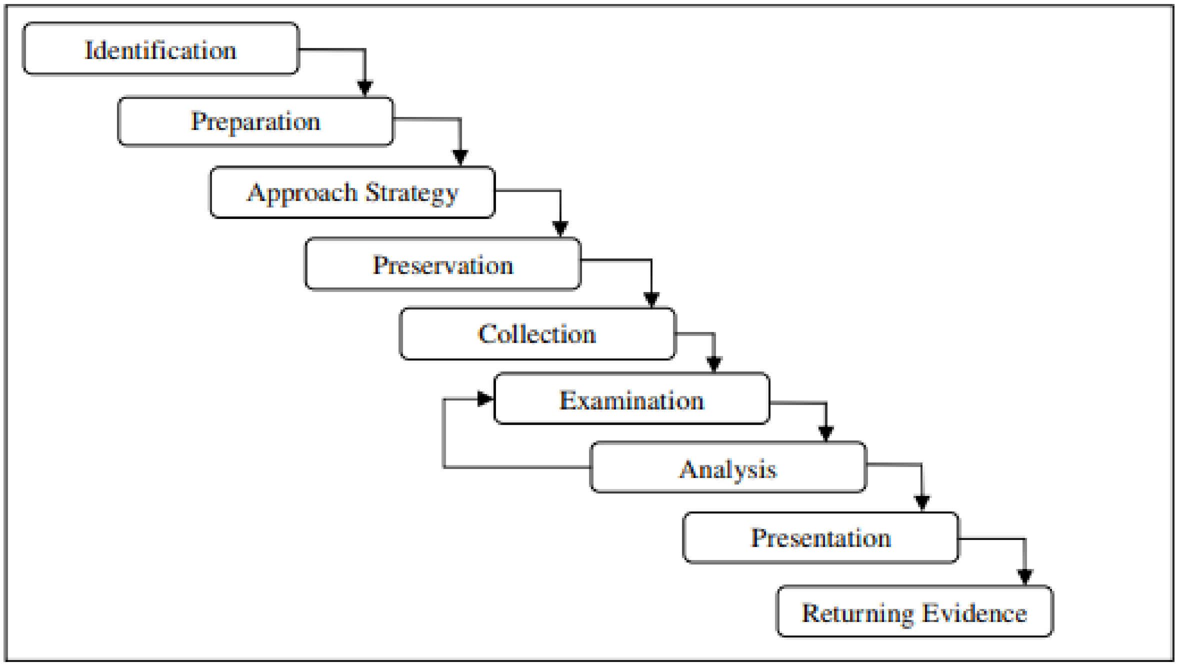


Figure 7: Abstract Digital Forensic Model *(Yunus Yusoff, June 2011)*.

After discussing how a digital forensic process is carried out in different scenarios, and now this study discusses some of the digital forensic tools.

Digital Forensic Tools

"Digital forensics depends on a kit of tools and techniques that can be applied equally to suspects, victims, and bystanders." (Garfinkel, 2017). As the days are passing, computers are becoming more advanced and powerful. This advancement leads to both good and bad, as finding the evidence from modern computers is becoming a tough task for the investigators. These computers contain an activity log of suspect's actions and words. Based on different scenarios, these tools can be categorized into different categories; they are:

- ❖ Internet analysis tools for internet browser analysis

- Network tools to analyze network IP addresses
- Tools to capture data from disk
- Tools to view and analyze files
- Tools to search in the database
- Mobile device analysis tools etc.

Amongst these categories, some of the tools are open source, and some tools should be purchased for advance functioning and performance. Some of the free, open-source digital forensic tools will be listed and discussed briefly below:

ProDiscover Basic

This tool is called a data recovery tool. If a computer is destroyed, and files are lost, ProDiscover basic helps to retrieve those files. An image file obtained from the evidence should be loaded to the tool before anything is done. If a computer is running with dual Operating Systems, sometimes there are chances that this tool can automatically select both the OS and provide data that is not required or part of the case. So, double-check, on which OS are you working or creating an image.

Not only recovering the data that is deleted, but this tool can also search for keywords which are relevant to the case . If an image file of 20GB or more has been extracted and loaded for analysis, then this keyword search helps in finding the required files, rather than wasting time searching for each and every file manually.

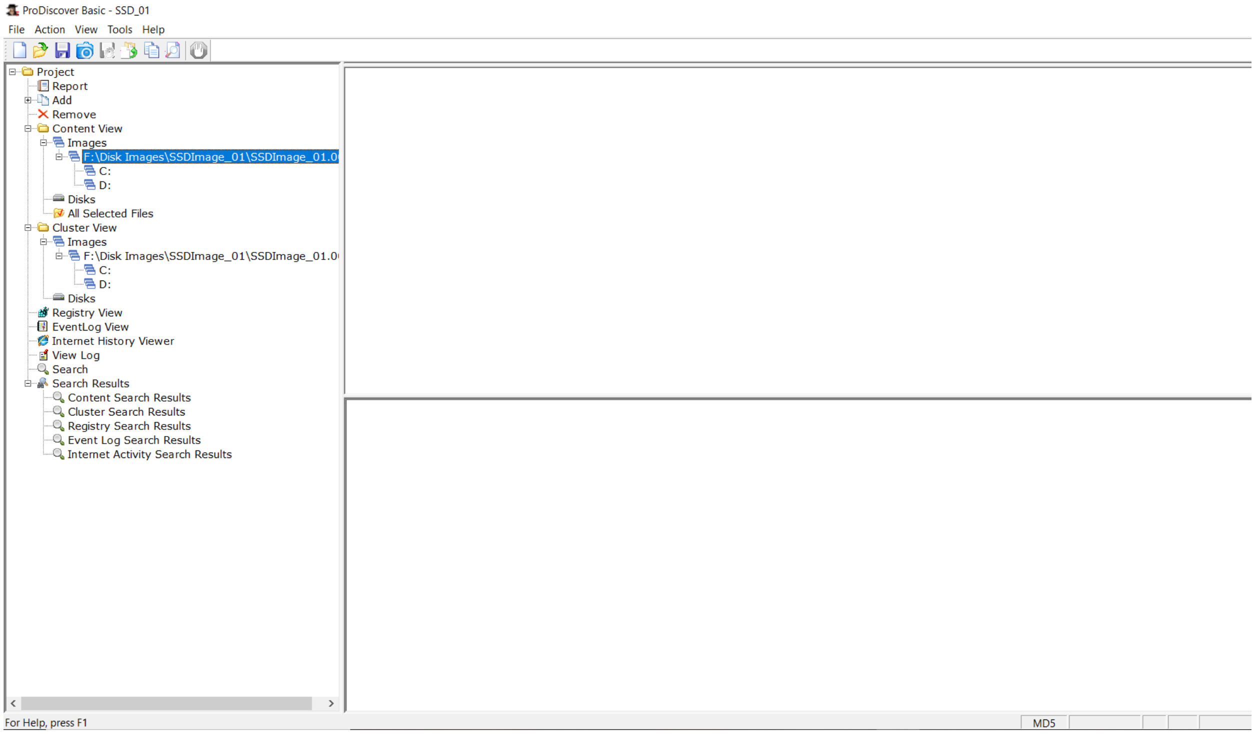


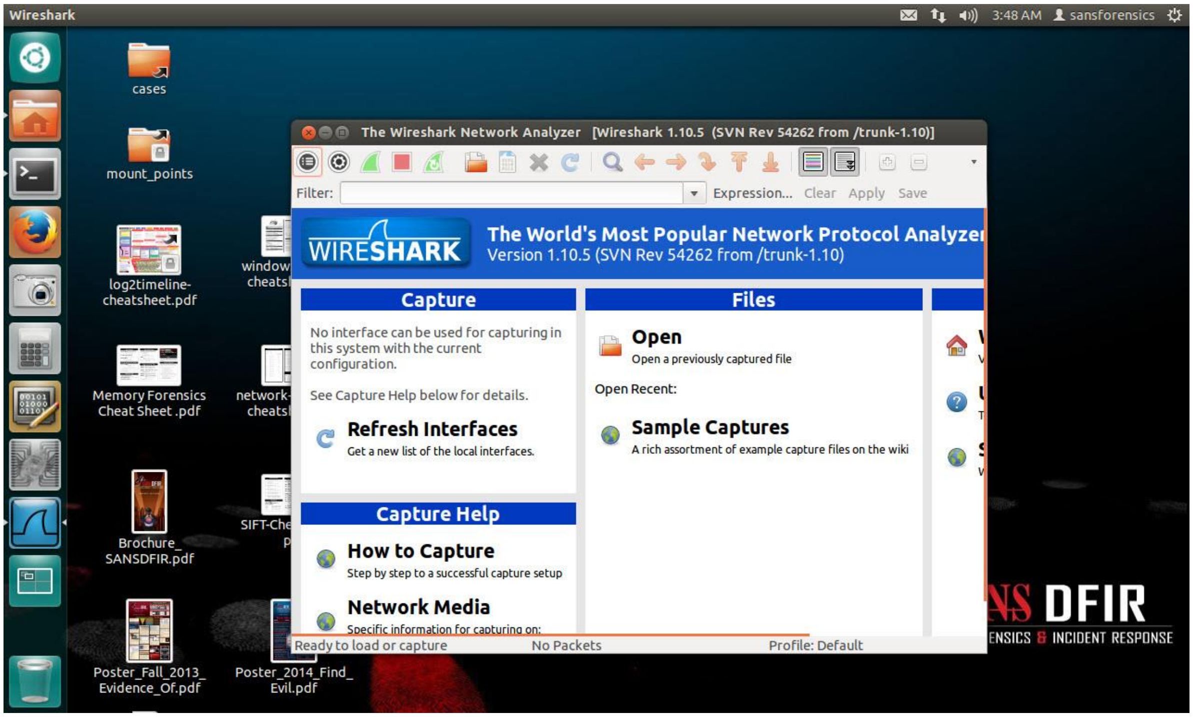
Figure 8: ProDiscover Basic tool.

The above figure 8 is a snippet from this study. This study uses the ProDiscover Basic tool to analyze the SSD image created using FTK Imager. This figure shows that an SSD image is added to the tool, and further, it is analyzed for deleted files and searched for keywords.

SANS SIFT

Commonly called SANS Investigative Forensic Toolkit (SIFT) is an Ubuntu-based Live CD. This is a very powerful tool built on Linux Ubuntu Operating System. This includes all the tools required to conduct a forensic or incident response investigation. Some of these tools are used to generate a timeline for system logs (log2timeline), carving a data file (Scalpel tool), recycle bin examination (Rifuiti), etc. This SANS SIFT supports different evidence formats like Advanced Forensic Format (AFF), Expert Witness Format (E01), and RAW (dd) format (SIFT

Workstation Download, n.d.). SANS SIFT provides documentation to understand the tools provided in it, which makes searching for evidence an easy process.


Wireshark
3:48 AM
sansforensics
cases
mount_points
log2timeline-cheatsheet.pdf
window cheats
Memory Forensics Cheat Sheet .pdf
network cheats
Brochure_SANSDFIR.pdf
SIFT-Che
Poster_Fall_2013_Evidence_Of.pdf
Poster_2014_Find_Evil.pdf
The Wireshark Network Analyzer [Wireshark 1.10.5 (SVN Rev 54262 from /trunk-1.10)]
Filter:
Expression...
Clear
Apply
Save
WIRESHARK
The World's Most Popular Network Protocol Analyzer
Version 1.10.5 (SVN Rev 54262 from /trunk-1.10)
Capture
Files
Refresh Interfaces
Open
Open Recent:
Sample Captures
Capture Help
How to Capture
Network Media
Ready to load or capture
No Packets
Profile: Default
NS DFIR
ENSICS & INCIDENT RESPONSE

No interface can be used for capturing in this system with the current configuration.

See Capture Help below for details.

Get a new list of the local interfaces.

Open a previously captured file

A rich assortment of example capture files on the wiki

Step by step to a successful capture setup

Specific information for capturing on:

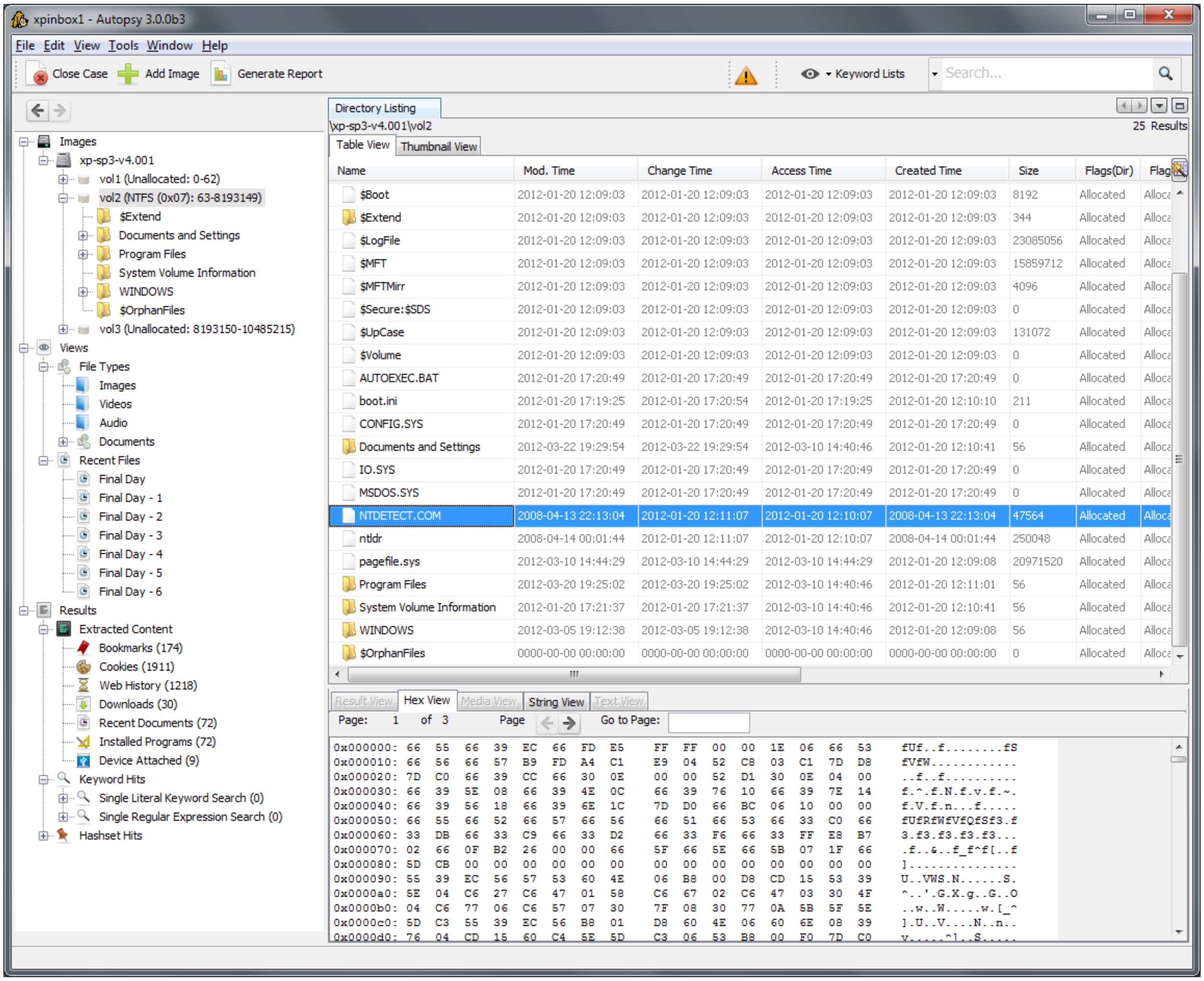
Figure 9: Wireshark network traffic analyzer tool in SANS SIFT *(Lee, 2014).*

Volatility

This tool supports memory dumps like raw dumps, crash dumps, VMWare dumps, etc. This tool analyzes RAM in 32-bit and 64-bit systems. This tool is based on python but can be run on different platforms like Windows, Linux, and Mac OS. Using this tool, we can extract open network socket information, running processes information, process ID’s, and many more (Balapure, 2018).

The Sleuth kit (+Autopsy)

This is an open-source digital forensics toolkit. This helps in analyzing the different file systems in detail. This tool has an additional Graphical User Interface (GUI) called Autopsy inside it. Features of this tool include hash filtering, file system analysis, keyword searching, and timeline analysis. Autopsy allows you to load an existing case or create a new one. A forensic image or a local disk is required to create a new case.



\xp-sp3-v4.001\vol2 25 Results

Name	Mod. Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flag
$Boot	2012-01-20 12:09:03	2012-01-20 12:09:03	2012-01-20 12:09:03	2012-01-20 12:09:03	8192	Allocated	Alloca
$Extend	2012-01-20 12:09:03	2012-01-20 12:09:03	2012-01-20 12:09:03	2012-01-20 12:09:03	344	Allocated	Alloca
$LogFile	2012-01-20 12:09:03	2012-01-20 12:09:03	2012-01-20 12:09:03	2012-01-20 12:09:03	23085056	Allocated	Alloca
$MFT	2012-01-20 12:09:03	2012-01-20 12:09:03	2012-01-20 12:09:03	2012-01-20 12:09:03	15859712	Allocated	Alloca
$MFTMirr	2012-01-20 12:09:03	2012-01-20 12:09:03	2012-01-20 12:09:03	2012-01-20 12:09:03	4096	Allocated	Alloca
$Secure:$SDS	2012-01-20 12:09:03	2012-01-20 12:09:03	2012-01-20 12:09:03	2012-01-20 12:09:03	0	Allocated	Alloca
$UpCase	2012-01-20 12:09:03	2012-01-20 12:09:03	2012-01-20 12:09:03	2012-01-20 12:09:03	131072	Allocated	Alloca
$Volume	2012-01-20 12:09:03	2012-01-20 12:09:03	2012-01-20 12:09:03	2012-01-20 12:09:03	0	Allocated	Alloca
AUTOEXEC.BAT	2012-01-20 17:20:49	2012-01-20 17:20:49	2012-01-20 17:20:49	2012-01-20 17:20:49	0	Allocated	Alloca
boot.ini	2012-01-20 17:19:25	2012-01-20 17:20:54	2012-01-20 17:19:25	2012-01-20 12:10:10	211	Allocated	Alloca
CONFIG.SYS	2012-01-20 17:20:49	2012-01-20 17:20:49	2012-01-20 17:20:49	2012-01-20 17:20:49	0	Allocated	Alloca
Documents and Settings	2012-03-22 19:29:54	2012-03-22 19:29:54	2012-03-10 14:40:46	2012-01-20 12:10:41	56	Allocated	Alloca
IO.SYS	2012-01-20 17:20:49	2012-01-20 17:20:49	2012-01-20 17:20:49	2012-01-20 17:20:49	0	Allocated	Alloca
MSDOS.SYS	2012-01-20 17:20:49	2012-01-20 17:20:49	2012-01-20 17:20:49	2012-01-20 17:20:49	0	Allocated	Alloca
NTDETECT.COM	2008-04-13 22:13:04	2012-01-20 12:11:07	2012-01-20 12:10:07	2008-04-13 22:13:04	47564	Allocated	Alloca
ntldr	2008-04-14 00:01:44	2012-01-20 12:11:07	2012-01-20 12:10:07	2008-04-14 00:01:44	250048	Allocated	Alloca
pagefile.sys	2012-03-10 14:44:29	2012-03-10 14:44:29	2012-03-10 14:44:29	2012-01-20 12:09:08	20971520	Allocated	Alloca
Program Files	2012-03-20 19:25:02	2012-03-20 19:25:02	2012-03-10 14:40:46	2012-01-20 12:11:01	56	Allocated	Alloca
System Volume Information	2012-01-20 17:21:37	2012-01-20 17:21:37	2012-03-10 14:40:46	2012-01-20 12:10:41	56	Allocated	Alloca
WINDOWS	2012-03-05 19:12:38	2012-03-05 19:12:38	2012-03-10 14:40:46	2012-01-20 12:09:08	56	Allocated	Alloca
$OrphanFiles	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Allocated	Alloca

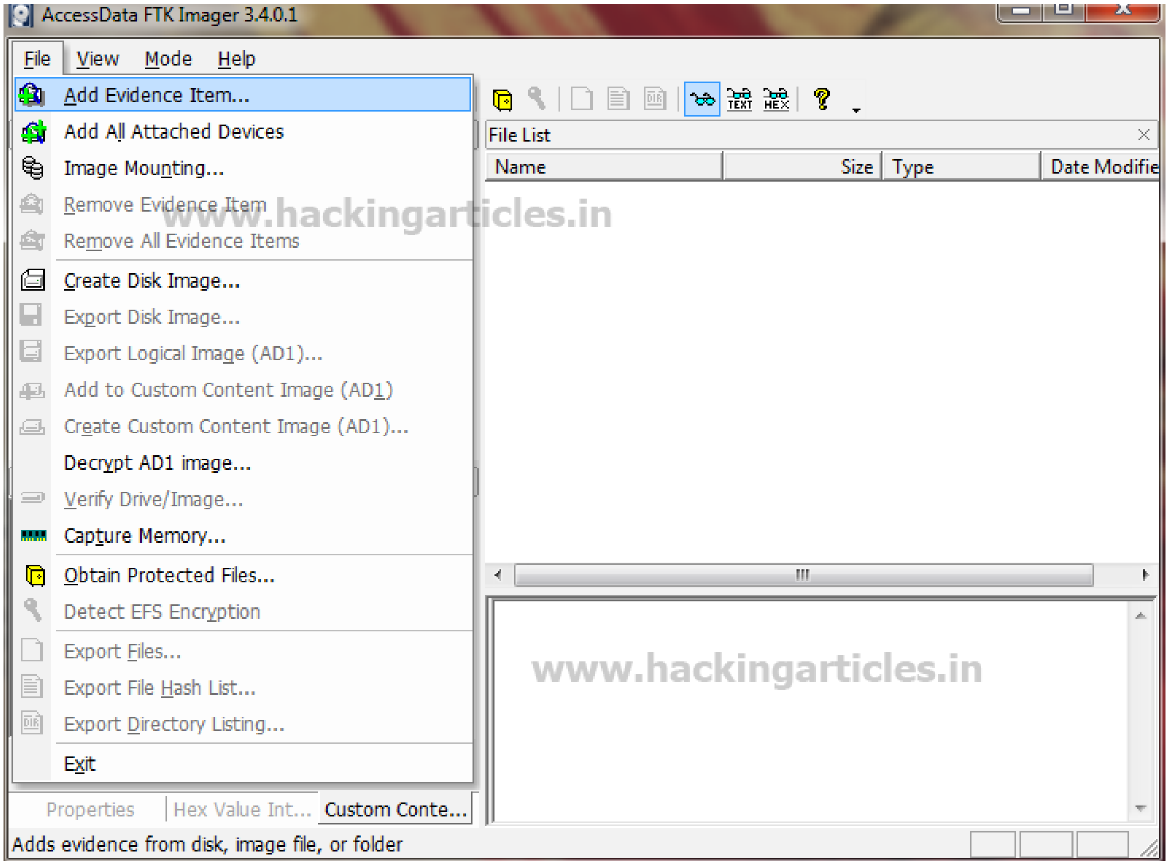
Page: 1 of 3 Page Go to Page:

```
0x000000: 66  55  66  39  EC  66  FD  E5    FF  FF  00  00  1E  06  66  53    fUf..f........fS
0x000010: 66  56  66  57  B9  FD  A4  C1    E9  04  52  C8  03  C1  7D  D8    fVfW............
0x000020: 7D  C0  66  39  CC  66  30  0E    00  00  52  D1  30  0E  04  00    ..f..f..........
0x000030: 66  39  5E  08  66  39  4E  0C    66  39  76  10  66  39  7E  14    f.^.f.N.f.v.f.~.
0x000040: 66  39  56  18  66  39  6E  1C    7D  D0  66  BC  06  10  00  00    f.V.f.n...f.....
0x000050: 66  55  66  52  66  57  66  56    66  51  66  53  66  33  C0  66    fUfRfWfVfQfSf3.f
0x000060: 33  DB  66  33  C9  66  33  D2    66  33  F6  66  33  FF  E8  B7    3.f3.f3.f3.f3...
0x000070: 02  66  0F  B2  26  00  00  66    5F  66  5E  66  5B  07  1F  66    .f..&..f_f^f[..f
0x000080: 5D  CB  00  00  00  00  00  00    00  00  00  00  00  00  00  00    ]...............
0x000090: 55  39  EC  56  57  53  60  4E    06  B8  00  D8  CD  15  53  39    U..VWS.N......S.
0x0000a0: 5E  04  C6  27  C6  47  01  58    C6  67  02  C6  47  03  30  4F    ^..'.G.X.g..G..O
0x0000b0: 04  C6  77  06  C6  57  07  30    7F  08  30  77  0A  5B  5F  5E    ..w..W.....w.[_^
0x0000c0: 5D  C3  55  39  EC  56  B8  01    D8  60  4E  06  60  6E  08  39    ].U..V....N..n..
0x0000d0: 76  04  CD  15  60  C4  5E  5D    C3  06  53  B8  00  F0  7D  C0    v.....^]..S.....
```

Figure 10: Autopsy tool interface *(Autopsy, n.d.)*.

FTK Imager

This is a data preview and imaging tool. This tool allows file and folder examination from local hard drives, CD/DVDs. We can also review a memory dump and forensic image content. Using FTK Imager, the files deleted can be recovered from the recycle bin. We can create hash values of files using MD5 and SHA-1 hashing algorithms. We can load an existing forensic image to view its contents (Tabona, 2018).



Adds evidence from disk, image file, or folder

Figure 11: FTK Imager – Adding new evidence *(Chandel, 2015)*.

There are many other free open source tools like CrowdStrike CrowdResponse, Linux ‘dd’, CAINE, DEFT, Xplico, etc.

Hard Disk Drive: Evolution and Properties

The first-ever commercial hard disk drive-based computer was introduced by IBM in 1956, and that was known as the Random-Access Method of Accounting and Control (RAMAC). Its HDD based storage system was called IBM 350 (Cohen, 2016). Surprisingly, to store data sixty years ago, it cost $650 per Megabyte/month. Relating to this cost, an iPhone would cost around $20 million a month to store data that wouldn't even sit in our pocket like today. Those days' hard disk drives are very big and too mechanical. These HDDs used to have magnetic disks and headers to read and write data. Later by 1960s and 1970s, personal computers (PCs) were introduced, which were huge and expensive. In 1980, a new start-up company introduced a 5 MB hard disk drive. This could easily fit in the PC, unlike old HDDs, which were as big as a refrigerator. The hard disk drive shrunk size was first compared to a refrigerator, then the size of the washing machine, and now it fits in a pocket. If we look back to the 1980s from now, the size variations of HHDs were 8 inches, 5.25 inches, 3.5 inches, 2.5 inches, 1.8 inches, and 1 inch (see figure 11 below). In later years, Solid-state drive was introduced, and all the drive-storage properties were dominated.

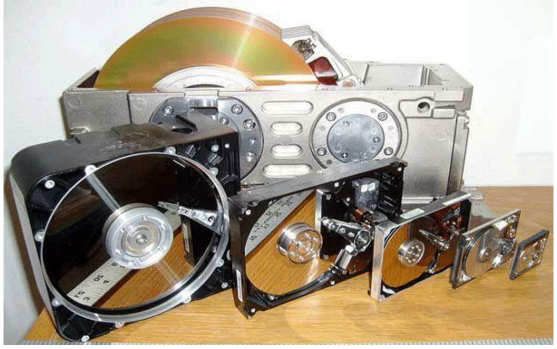


Figure 12: HDD size variations from the 1980s – Present days *(The evolution of hard disk drives, 2019)*

Solid State Drive: Evolution and Properties

The solid-state drive was first produced in the 1950s. These were mostly RAM-based. It came out in two technologies: Card Capacitor Read-Only Store (CCROS) and magnetic core memory. For early IBM in the 1970s and 1980s, semiconductor memory SSDs were implemented. The Bulk core was a product that was produced in the 1970s by Dataram. This could provide only 2 MB of RAM solid-state storage. In the year 1978, a 16 KB solid-state drive was produced by Texas Memory Systems, which were used by oil companies (Romano, 2014). Later in the early 1980s, 128 KB, solid-state storages were used. From Kilobytes, they slowly moved onto more storage space (Megabytes), where 20 MB solid-state storage was built-in with 40 MB tape memory.

Later in 1988, the world's first flash-based Solid-state drive was prototyped by Digipro (PC vendor, Alabama-based). It took a couple of years for the product to be functioning and shipped. Different size capacities were produced like 2 MB, 4 MB, 6 MB, and 8 MB. It was very expensive those days, the high-end model being sold for $5000. Later by the year 1995, the modern flash-based drive took birth. They named it as FFD (Fast Flash Disk). Their capacity ranged from 16 MB – 896 MB. By the year 2003, cheaper flash-based SSDs were introduced by Transcend Company. In those days, this technology was only restricted to cameras. Later in 2006 and 2007, both Samsung and SanDisk introduced a 2.5-inch 32 Gigabyte drive with a Parallel ATA interface standard (Edwards, 2012). People realized that new SSD technology is so fast, and by the end of 2008, sales started to increase. So many technology companies started to push SSD to its limits. Year by year, SSDs are getting faster and cheaper. A 160 GB capacity SSD has a read speed of 270 MBps (Megabytes per second) and costs around $300, which is not expensive compared to a decade from the past. The future of SSD is, it can be produced in many new forms with high read/write speeds, more capacity, and high durability.

Table 2

Differences between HDD and SSD (R, n.d).

PARAMETER	Hard Disk Drive (HDD)	Solid State Drive (SSD)
Components	Contains moving mechanical parts, like the head to read and write data.	Does not contain moving mechanical parts. Contains electronic parts like ICs.
Read/Write Time	Has longer R/W time.	Has shorter R/W time.
Latency	Has higher latency.	Has lower latency.
I/O operations per second	Supports less I/O operations per second.	Supports more I/O operations per second.
Weight	Heavier in weight.	Lighter in weight.
Size	Larger in size.	More compact in size.
Data Transfer	Data transfer is sequential.	Data transfer is random access.

Reliability	HDD is less reliable due to the possibility of mechanical failure, like head crash and susceptibility to strong magnets.	More reliable.
Cost	Cheaper per unit storage.	Expensive per unit storage.
Time of Release	Older and more traditional.	Recent, advanced and comfortable to use.
Noise	Can produce noise due to mechanical movements. Noisier.	Does not produce any noise.

Summary

This chapter discussed the background and literature research required for a better understanding of this study. Started off discussing what forensics is and types of forensics. Detail description about digital forensics and its process from the evidence-gathering phase to the results analysis phase. Later different tools used in digital forensics are listed and explained briefly. A table differentiating SSD and HDD is discussed, and the next chapter explains the methods followed in conducting this study.

Chapter III. Methodology

Introduction

This chapter includes the design flow of how the experiment is carried out, methods involving procedures, requirements, etc. all of which are a part of this research. The tools used, drives used, devices used, and names of the image files generated from these drives will be listed and discussed. Specifications and requirements of the devices used will also be discussed. So basically, this chapter tells us more about how the experiment is going to be conducted, and this can be understood starting with the design of this experiment.

Design of the study

This research is basically a comparison between the Solid-state drive forensics and Hard disk drive forensics. When it says forensics comparison, it means that different forensic tools are used to analyze and understand the behavior of the drives. On performing this, we can understand how typical the job of a forensic investigator is, dealing with different types of data storage devices, i.e., drives (SSD, HDD). The first step in this will be creating a case scenario. This is nothing but a set of data files that will be created and stored on the investigator's laptop, where all the forensic tools will be installed, and the experiment is carried out. These case folder and folders inside it can contain any kind of random data like images, documents, excel sheets, etc. Later this Dummy case folder will be copied to respective SSD and HDD. Three open-source forensic tools FTK toolkit/ FTK Imager, Autopsy, and ProDiscover Basic, will be used in this research experiment. To extract the images of the drives, before and after deleting evidence data files from the dummy case folder, the FTK Imager forensic tool will be used. The first image is captured before deleting any data from the case folder, and some specific data files will be deleted on both the drives; the second image file will be created after the deletion using the FTK toolkit. Later as an optional practice, both the drives can be formatted, and another copy of the image can be created (This is optional). After these two image files are created for each drive, these image files will be loaded in Autopsy forensic tool to view and analyze the results. These images can also be loaded in the FTK toolkit for analysis, but Autopsy is an advanced tool with a good user interface and helps us in understanding more about the deleted files and any keyword search if done. Using Autopsy forensic tool, one can search for keywords, deleted files, deleted images, image source, and image location, etc. As mentioned, the third forensic tool used in this research is ProDiscover Basic; this will be used to recover and view the deleted files from both the drives similar to Autopsy. The reason behind using another similar tool is to observe if there will be any difference in the behavior of the drives when analyzing for deleted files and keyword searches.

The image files created from the FTK imager will be in a raw “dd” format. This format represents a data dump, i.e., a dump of all the data in the drive. A fresh image will be extracted from the drives using ProDiscover Basic with a “.eve” file extension. Image files with this “.eve” extensions are loaded into ProDiscover Basic for analyzing the respective drives. Instead of capturing the image of SSD and HDD for multiple times, raw dd format can also be used. To clearly understand the behavior of these drives when analyzed in the ProDiscover Basic tool, a default “.eve” image file is created and analyzed.

All the steps listed above will be presented in the figure below. Figure 9 is a design flow of the whole experiment, where the drives involving in the case will be identified as the first step of the investigation, and a dummy case folder is created. This folder is copied to the drives for extracting images before and after deleting files that act as evidence related to this case. The extracted images will be loaded, analyzed using different forensic tools, and results are compared to get the conclusion of this experiment.

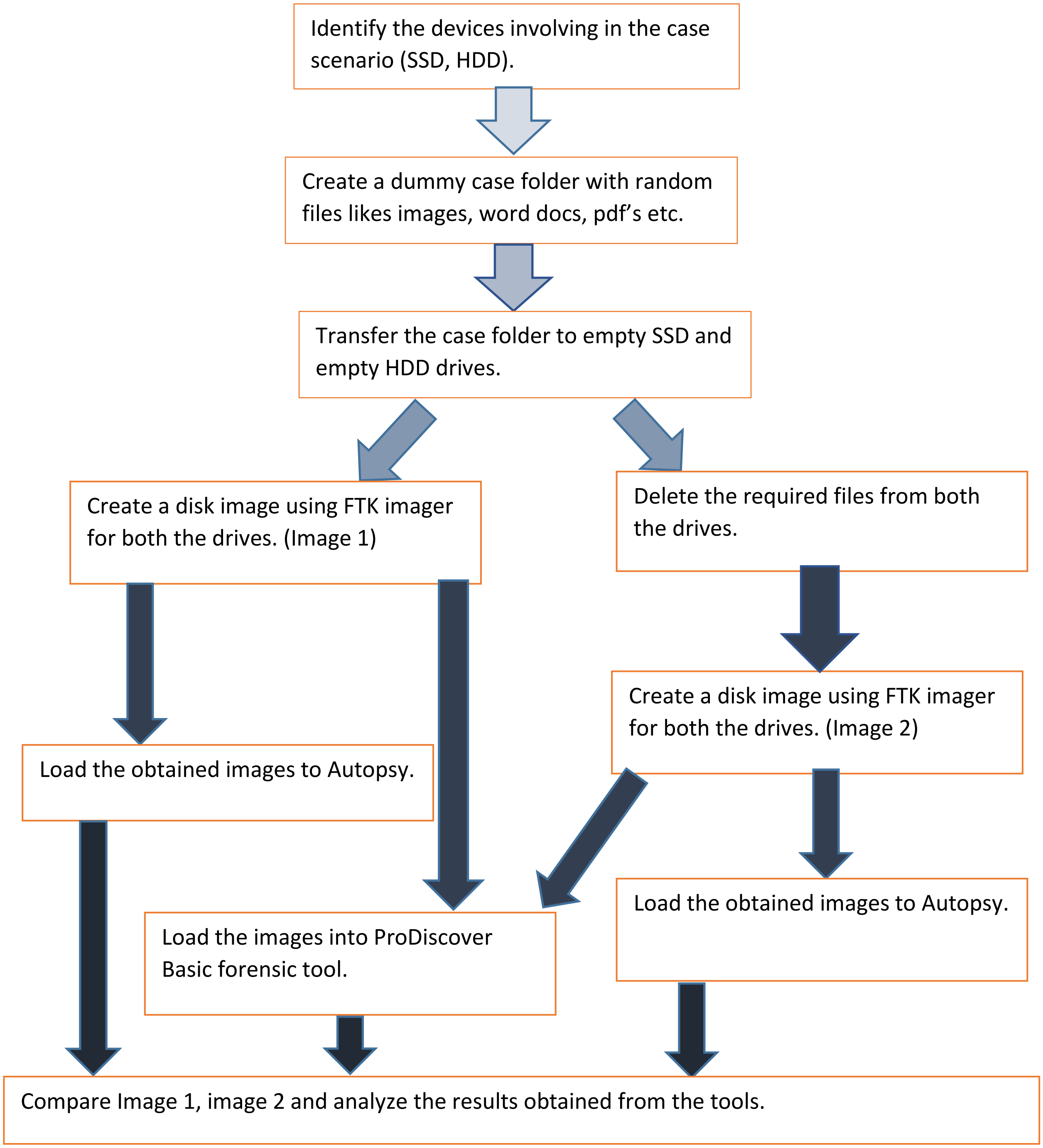

Identify the devices involving in the case scenario (SSD, HDD).
Create a dummy case folder with random files likes images, word docs, pdf’s etc.
Transfer the case folder to empty SSD and empty HDD drives.
Create a disk image using FTK imager for both the drives. (Image 1)
Delete the required files from both the drives.
Create a disk image using FTK imager for both the drives. (Image 2)
Load the obtained images to Autopsy.
Load the images into ProDiscover Basic forensic tool.
Load the obtained images to Autopsy.
Compare Image 1, image 2 and analyze the results obtained from the tools.

Figure 13: Design flow of experiment.

Data Collection Model

This study analyzes the results obtained from two different storage devices; they are an external hard disk drive with a storage capacity of 1 TB and an external solid-state drive with a storage capacity of 120 GB. The image files created by the FTK Imager will be of ".001" file extension. The image files created can be named as you wish. Thus, an investigation will be conducted on these image files expecting a result in favor of either SSD or HDD. The additional hardware required for conducting this research would be an investigator laptop, i.e., a laptop loaded with FTK toolkit, Autopsy forensic tool, and ProDiscover Basic forensic tool. All the image creation and evidence analysis will be done on the investigator's laptop. There are no specific mandatory requirements for the investigator's laptop. It can run Windows Operating System with a processor of i5 or i7. Since it will take a lot of time to create drive images, it is suggested to have a good working laptop with better processing speeds.

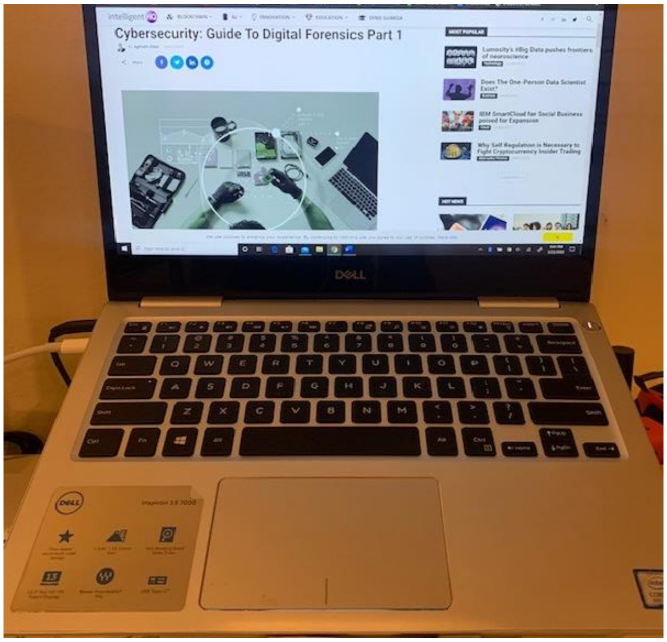


Figure 14: Investigator laptop.

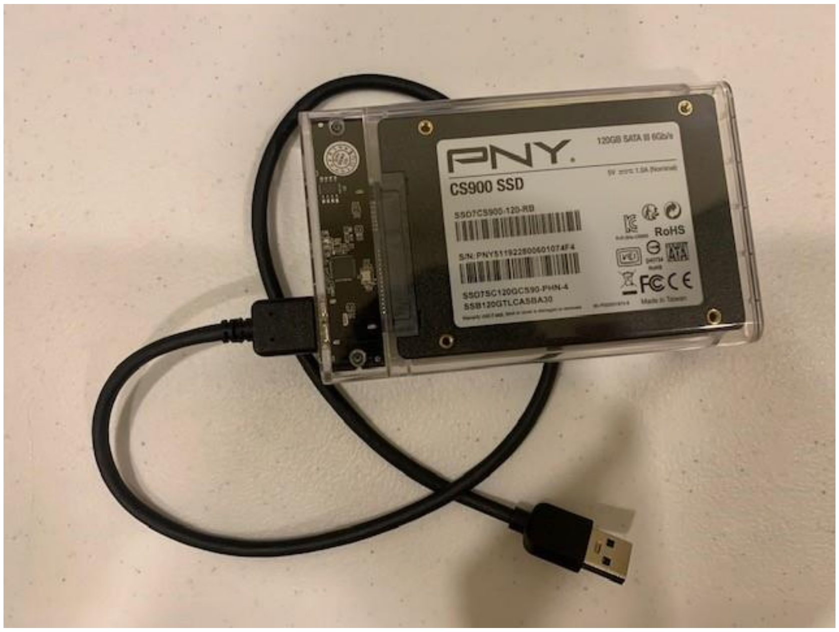


Figure 15: Solid State Drive with 120 GB storage.

Figures 15 and 16 are the Solid-state and Hard disk drives used in this experimental study. The specifications like read/write speed, storage capacity, manufacturer details, supported file systems, etc. will be tabulated below.

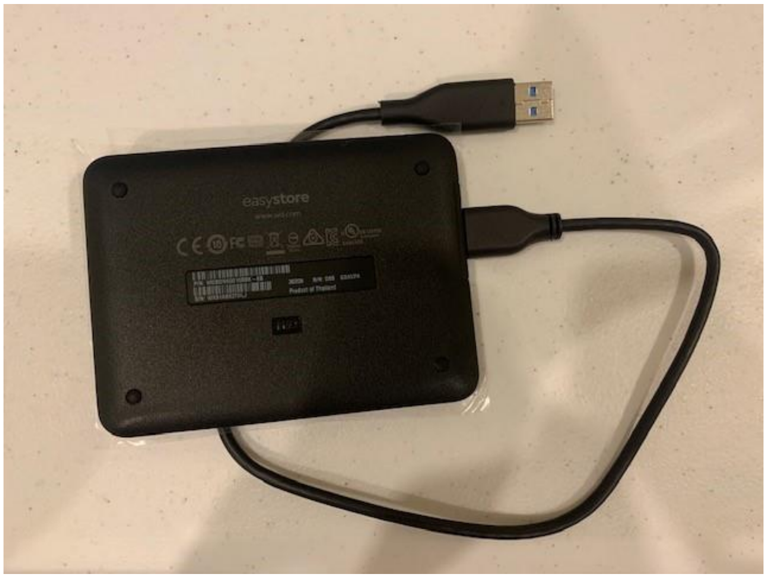


Figure 16: Hard Disk Drive with 1 TB storage.

Table 3

Storage devices and their specifications.

Type	Solid State Drive	Hard Disk Drive
Make/Model	PNY CS 900	WD - Easystore
Storage capacity	120 GB	1 TB
Read speed	200 MB/s	80 MB/s
Write speed	500 MB/s	160 MB/s
Supported file systems	FAT 32, NTFS	FAT 32, NTFS, exFAT
Hardware Connectivity	SATA III	USB 3.0
Access speeds	0.1 ms	5.5 ~ 8.0 ms

Table 3 above tabulates all the specifications of both the drives, which are to be observed to conduct this study. As we all know, SSDs have better read/write speeds than HDDs; it can be clearly seen in the table. Similarly, access speeds of SSD are dominant compared to HDD. Rest all specifications listed are common and can be understood with basic knowledge of understanding. These are the devices/drives that are used in this study for data collection.

The first thing to be remembered before even starting the experiment is to wipe out any kind of data that is present on the storage drives. It is always suggested to format the drives for better results. Created dummy case folder should be copied to these empty SSD and HDD drives. Two image files are extracted from both SSD and HDD using FTK Imager tool. Image created from SSD is saved as “SSDImage_01” and from HDD is saved as “HDDImage_01”. After deleting evidence data from both drives, two more images are extracted. These extracted images are saved as “SSDImage_2” and “IMGHDD_2” respectively. The other tool used for creating images after deleting evidence data from drives is ProDiscover Basic. As it was taking more than 46 hours to create an image of a 1 TB hard drive using this tool, an image of SSD was created, excluding HDD image. Many studies have experimented and proved that using the ProDiscover Basic forensic tool, deleted data on Hard drives can be identified and retrieved. Hence this study concentrates more on identifying and retrieving deleted data on Solid-state drives. The SSD image created using ProDiscover Basic is saved as “ProDiscSSD_Image.eve.” This is more about how data is collected and saved for this study to be conducted. Images created from FTK Imager will be analyzed using Autopsy, and Images created from ProDiscover will be analyzed in the same tool itself. The next section will discuss about the software tools and techniques used in this study.

Tools and Techniques

The software tools and techniques used for this study are discussed here. For this forensic investigation to be carried out, different forensic tools are used. The most important tool in this investigation is the FTK toolkit. Forensic Toolkit (FTK) is a computer forensic software developed by AccessData (N.D, 2019). This FTK toolkit has a standalone tool known as FTK Imager. This FTK Imager plays a key role in capturing all the images analyzed in this study. Basic functionalities of Forensic Toolkit are searching for keywords, locate deleted files, search for deleted emails, files, etc. The tool used to analyze the images extracted using FTK Imager is Autopsy – The Sleuth kit. This is also a computer forensic software similar to FTK serving a different purpose, i.e., analyzing the image (Carrier, 2020). This tool is compatible with analyzing the images extracted from NTFS, FFS, FAT, and EXT2FS file systems. To understand a little bit more about the behavior of SSD, the other tool used is ProDiscover Basic. This is an advanced data recovery tool that has a feature of displaying data diagnostics. Data that is hidden or deleted can be retrieved, and keyword search is faster compared to another computer forensic software's. This tool is used for extracting the image of SSD, and the same image is used for analyzing in this tool. These are the computer forensic tools used in conducting this study. Moving on to the hardware and software requirements for this study to be conducted.

Hardware and Software Requirements

In order to perform a forensic investigation, every investigator has some basic hardware and software requirements. The requirements gathered for this study and their versions are tabulated below. The versions mentioned are not restricted to all forensic investigations; those are just what has been used in this study.

Table 4

Software and Hardware requirements.

Software Requirements:

1. Forensic Toolkit version 7.1.0 – Computer Forensic Software
2. FTK Imager version 4.2.1 – Computer Forensic Software
3. Autopsy version 4.14.0 - Computer Forensic Software
4. ProDiscover Basic version 7 - Computer Forensic Software

Hardware Requirements:

1. Investigator laptop – Dell Inspiron 13 7370 – 8th Gen i5 Processor
2. PNY CS 900 external SSD - 120 GB SATA III
3. WD Easystore external HDD – 1 TB, 4 TB

Summary

This chapter started discussing about the design flow of the experiment with a good flow chart, which is nothing but what this study basically does. This chapter has also covered a little bit about how the data is collected from SSD and HDD using FTK Imager, with the specific extracted image names being declared. These extracted images are analyzed by loading into Autopsy and ProDiscover basic tools. The differences and specifications between the SSD and HDD used in this experiment are tabulated. Later the tools and techniques required for this experiment are listed, and finally, the hardware, software requirements gathered are listed in a table. The next chapter discussed more in-depth about how the whole experiment is carried out by presenting the data and analyzing the images extracted for better understandings.

Chapter IV. Data Presentation and Analysis

Introduction

In general, a forensic investigator gathers all the evidence involving in a case scenario and starts extracting images from the respective drives. These extracted images will be analyzed loading into specific computer forensic tools. Similarly, this chapter tells more about how and what type of data is collected and presented to different forensic tools used in this study. In detail explanation of how images can be extracted is clearly represented with the appropriate figures in a step by step order. These extracted images will then be subjected to different forensic tools for analysis. Next section explores on how this study is conducted with more figures and their explanations.

Data Presentation

To perform this study, a dummy case folder is created. Some random image files, word files, and a pdf doc file, are added to this dummy case folder, which acts as evidence to a case. The data present in this dummy folder is not related to any real-life case scenarios. It is just an assumption made for a better understanding of the study. Each step involved in this process is discussed below.

Creating a dummy case folder

A dummy case folder is created in the investigator's laptop, and some random files from the web are added to it. This case folder contains subfolders and different files in it. In detail, this case folder has three subfolders “Victim’s car,” “Victim’s house,” “Victim’s face,” and four other images, “Travel info.xlsx” is an excel sheet which has data of the person involving in the case has traveled to. A word file “victim’s identifications.docx,” a pdf file “DateofAction.pdf,” are a part of this case folder. To make it a little bit interesting, a case scenario is imagined similar to the real-time digital forensic cases. The case assumed here is a murder case, and the files added to the folder are related to it. Figure 17 has all the folders and files in the dummy case folder.

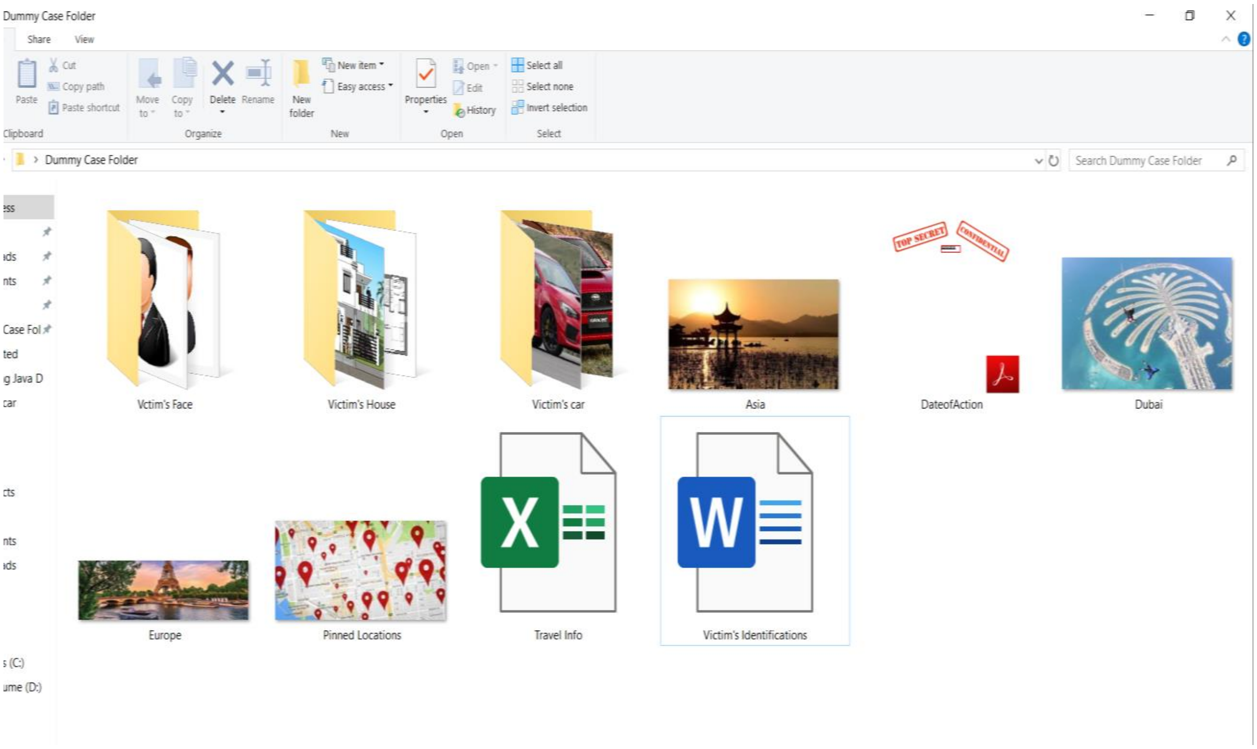


Figure 17: Dummy Case Folder.

The murder case scenario assumed here exactly is, a person who plans for a murder collected all the details related to the victim like a victim ‘s face pictures, house pictures, car pictures, etc. All the folders and their contents are expanded and explained in the below figures.

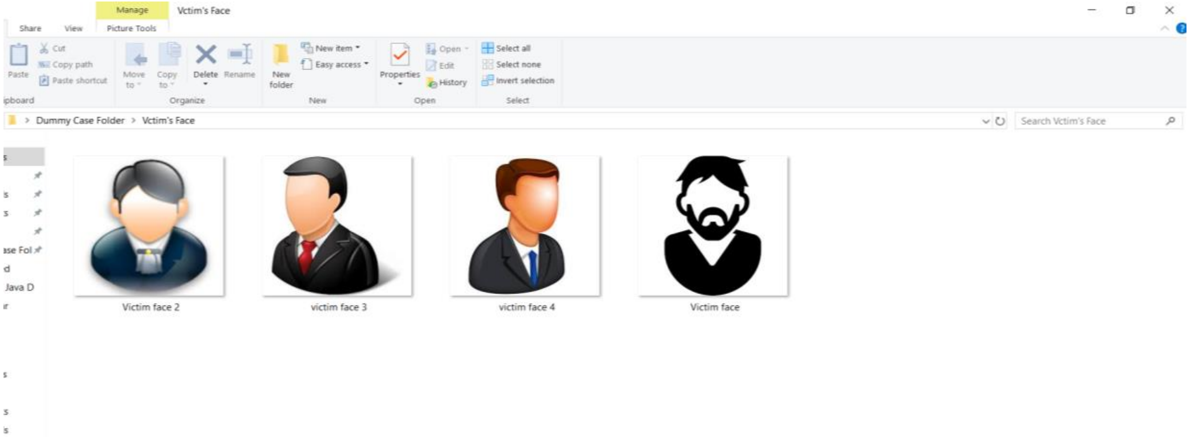


Figure 18: Victim's face folder images.

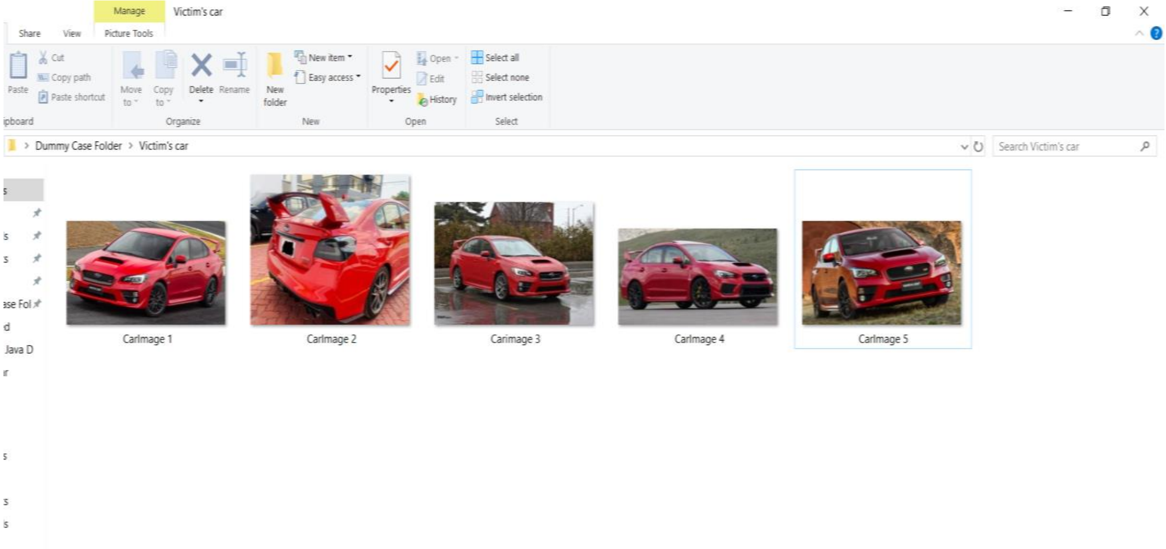


Figure 19: Victim's car folder images.

The above two figures 18 and 19 have pictures being clicked from different angles. Front angle, side angle, back angle for face and front view, rearview, side view, license plate view, etc. for car pictures. These pictures from different angles make the job easy for the person planning the murder. Figure 20 below has a victim’s house image and a blueprint image of that house. Having a street number alone sometimes is not enough to find the house these days, so it is better to have a house picture to locate easily. There is also a blueprint image; this blueprint helps the murderer to plan his murder more accurately and have an escape plan out of it.

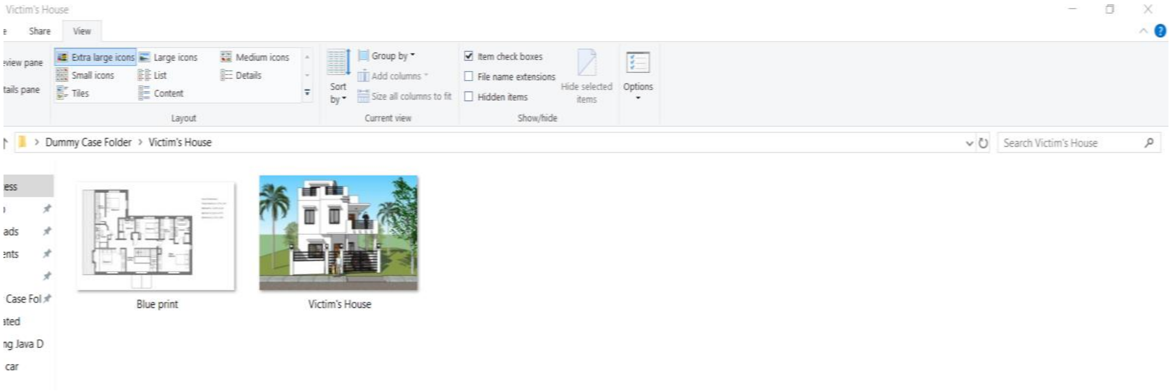


Figure 20: Victim's house folder images.

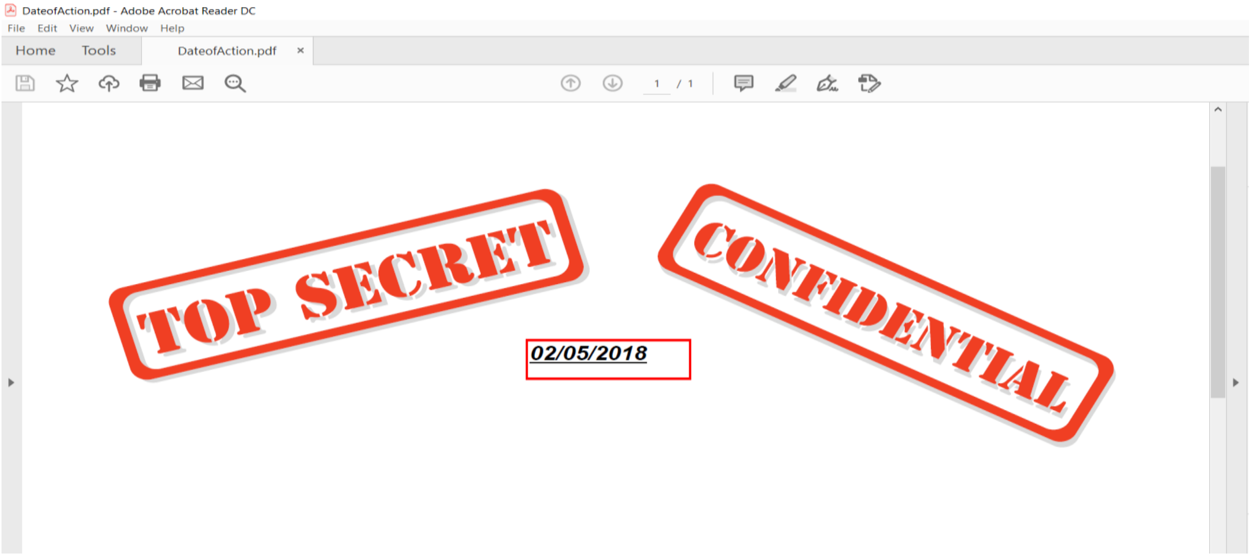
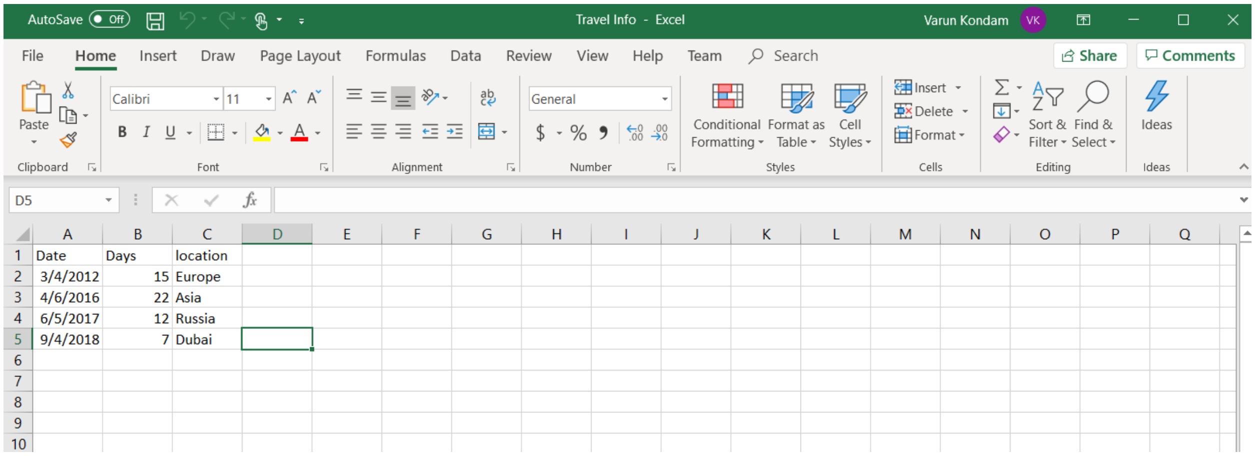

DateofAction.pdf - Adobe Acrobat Reader DC
File Edit View Window Help
Home
Tools
DateofAction.pdf
1 / 1
TOP SECRET
CONFIDENTIAL
02/05/2018

Figure 21: “DateofAction.pdf” file content.

Figure18 is a pdf file with the name “DateofAction.pdf,” and this file is marked as a top-secret and confidential for the case because, as this has the final date, i.e., 02/05/2018. This final date is the date on which the murder has been planned. The figure below is just a piece of random travel information that is included in the case folder. This is added as a support file to the case folder and is not related nor acts as evidence to the assumed murder case.

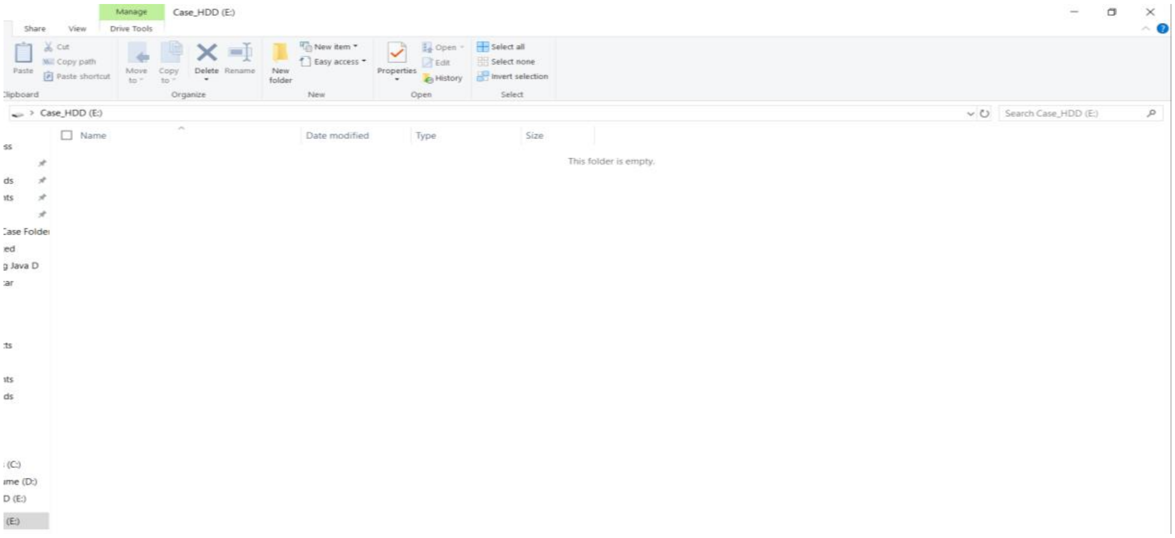

AutoSave Off
Travel Info - Excel
Varun Kondam
File Home Insert Draw Page Layout Formulas Data Review View Help Team Search
Share
Comments
Clipboard Font Alignment Number Styles Cells Editing Ideas
D5

	A	B	C	D
1	Date	Days	location	
2	3/4/2012	15	Europe	
3	4/6/2016	22	Asia	
4	6/5/2017	12	Russia	
5	9/4/2018	7	Dubai	

Figure 22: Travel info excel sheet data.

Copying the case folder to HDD and SSD

Figure 23 shows that the 1 TB external Hard drive required for this experiment is named as “Case_HDD,” and the drive is emptied to confirm there are no previous data files in it. It is always good to wipe out the drive before loading any case data into it for better results.



This folder is empty.

Figure 23: Formatted external HDD drive.

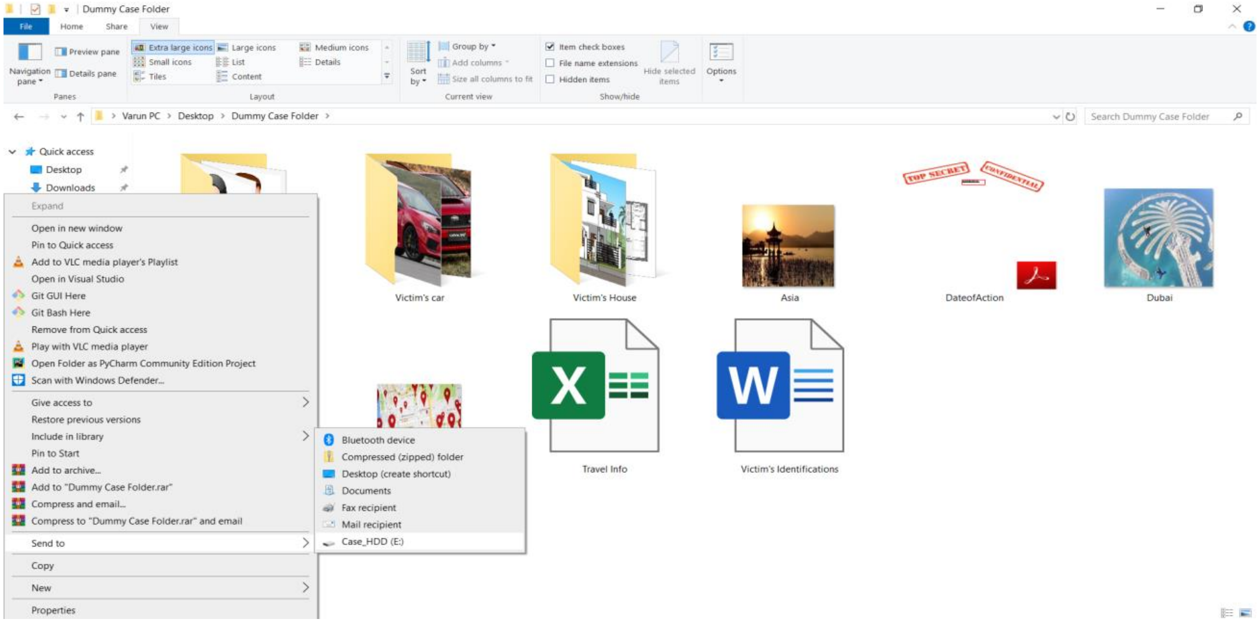
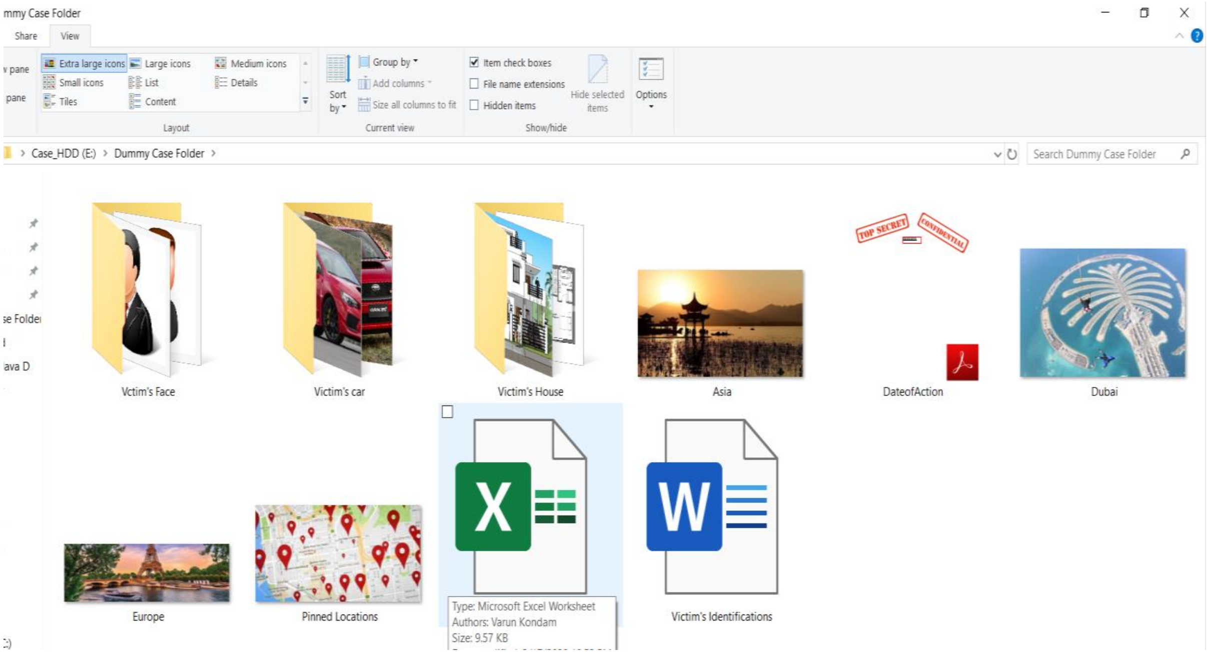


Figure 24: Loading case folder to HDD.

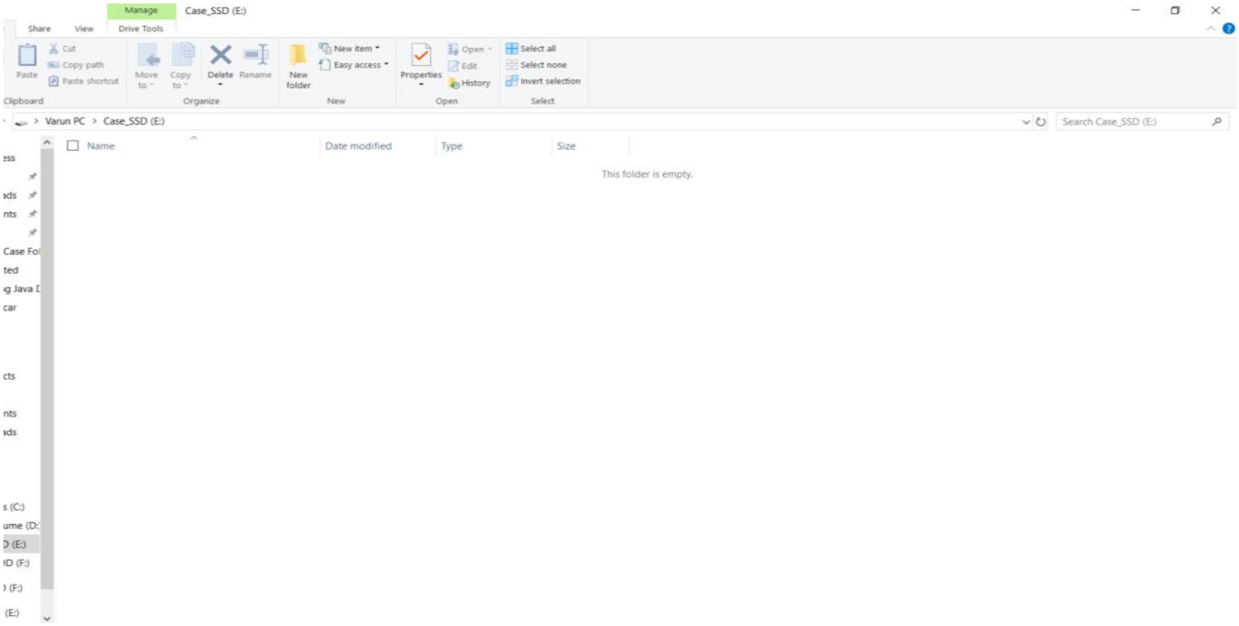
Figures 24 and 25 shows that case files from “Dummy Case Folder” are copied to the destination “Case_HDD” external Hard drive. After copying the case files to external Hard drive, double-check to make sure that all files have been copied or not.



Type: Microsoft Excel Worksheet
Authors: Varun Kondam
Size: 9.57 KB

Figure 25: Case files in Hard Disk Drive.

Figure 26 shows an empty SSD drive named “Case_SSD.” Similarly, after copying case folder to HDD, SSD is formatted to completely wipe out any previous data files present on it.



This folder is empty.

Figure 26: Empty External SSD drive.

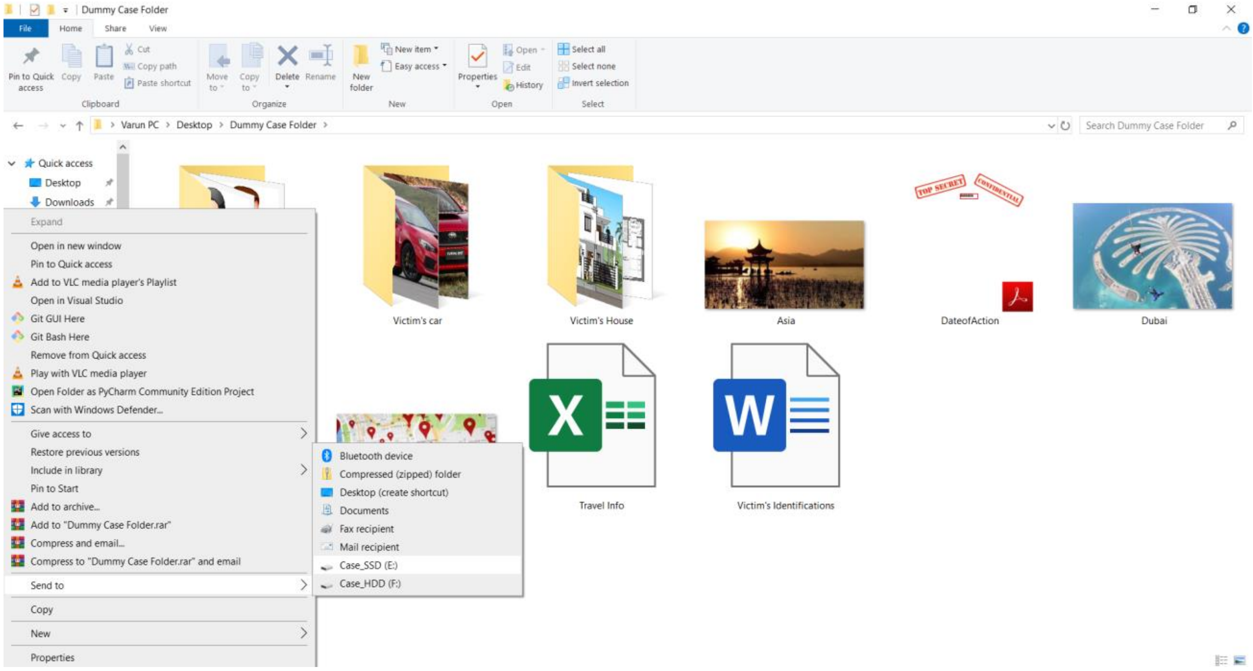


Figure 27: Loading case folder into SSD.

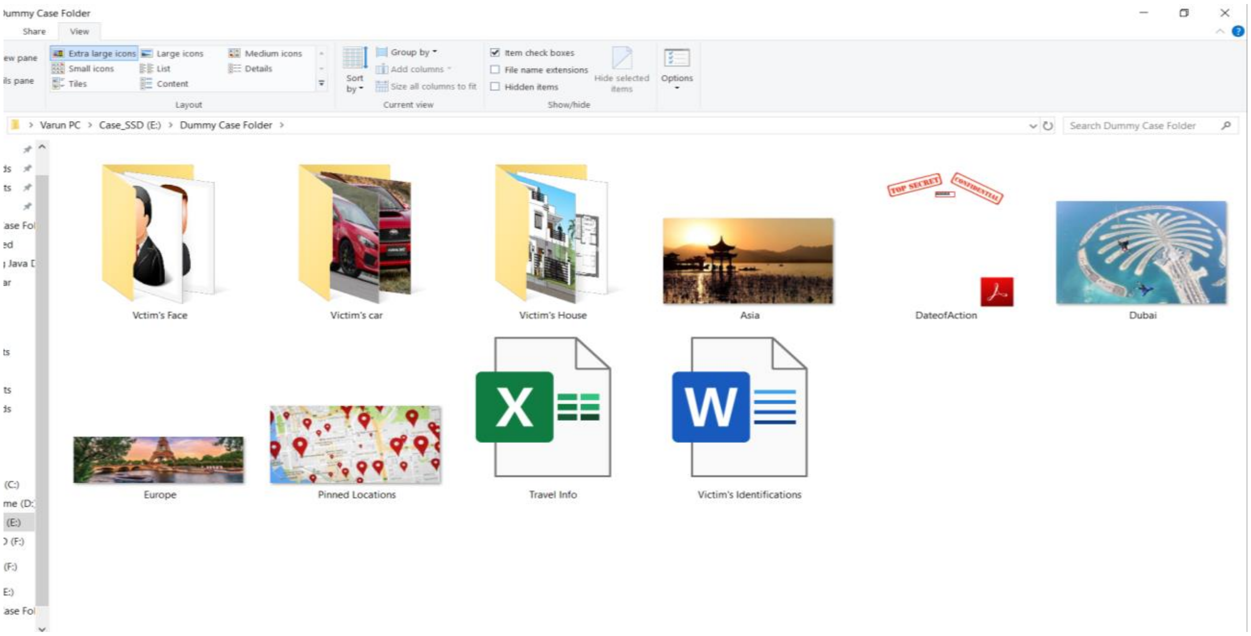
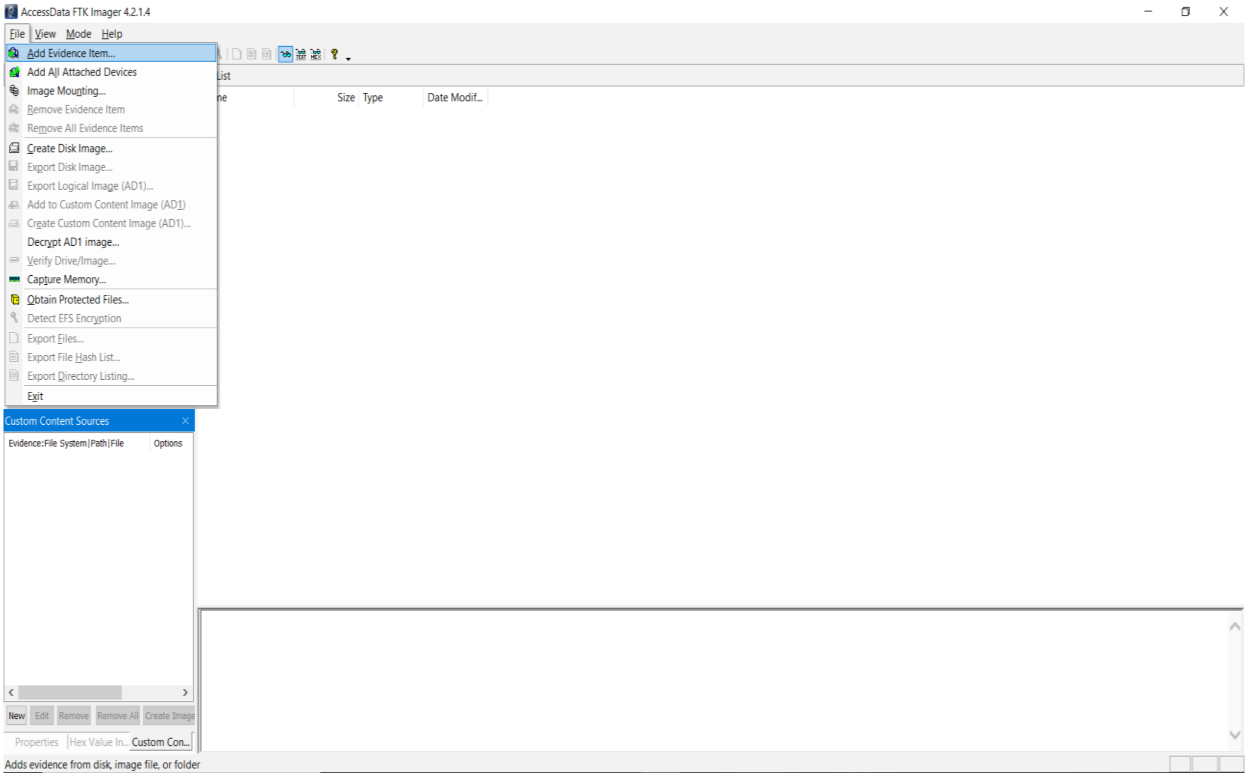


Figure 28: Case files in Solid State Drive.

This is how the dummy case folder created on the investigator laptop is copied to the respective SSD and HDD. The next step in this process will be extracting images from these two drives using FTK Imager.

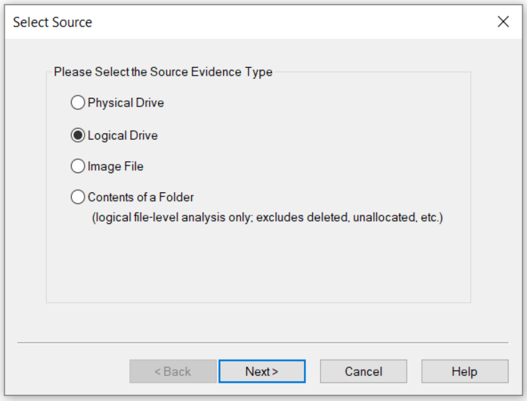
Phase 1 - Extracting images from SSD and HDD (Before Deleting files):

After the case folder is created and copied to SSD, HDD; image files are extracted. Creating image files using FTK Imager before deleting any evidence files from the drives is considered as phase 1 for this study. SSD image creation is shown below, step by step.



Adds evidence from disk, image file, or folder

Figure 29: Adding evidence to FTK Imager.



Please Select the Source Evidence Type

○ Physical Drive

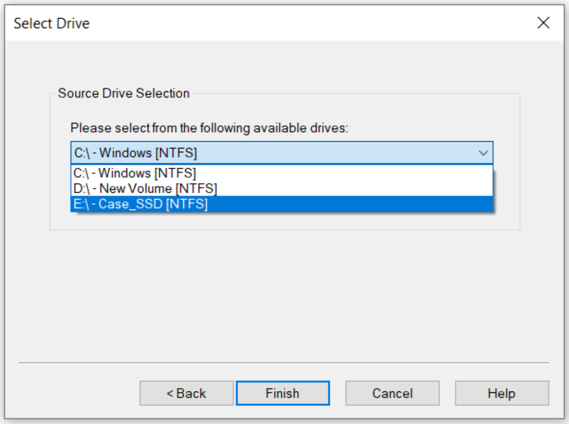
● Logical Drive

○ Image File

○ Contents of a Folder
(logical file-level analysis only; excludes deleted, unallocated, etc.)

Figure 30: Selecting the source drive type.

From Figure 30, make sure to select the right source evidence drive type, i.e., Physical drive/ Logical drive. Since the Hard Disk Drive has mechanical moving parts and it stores data by writing into a magnetic disc, it is selected as a physical drive; conversely, Solid-State Drives read and write data logically, they are selected as logical drives. Select Logical Drive and then click on Next.



Source Drive Selection

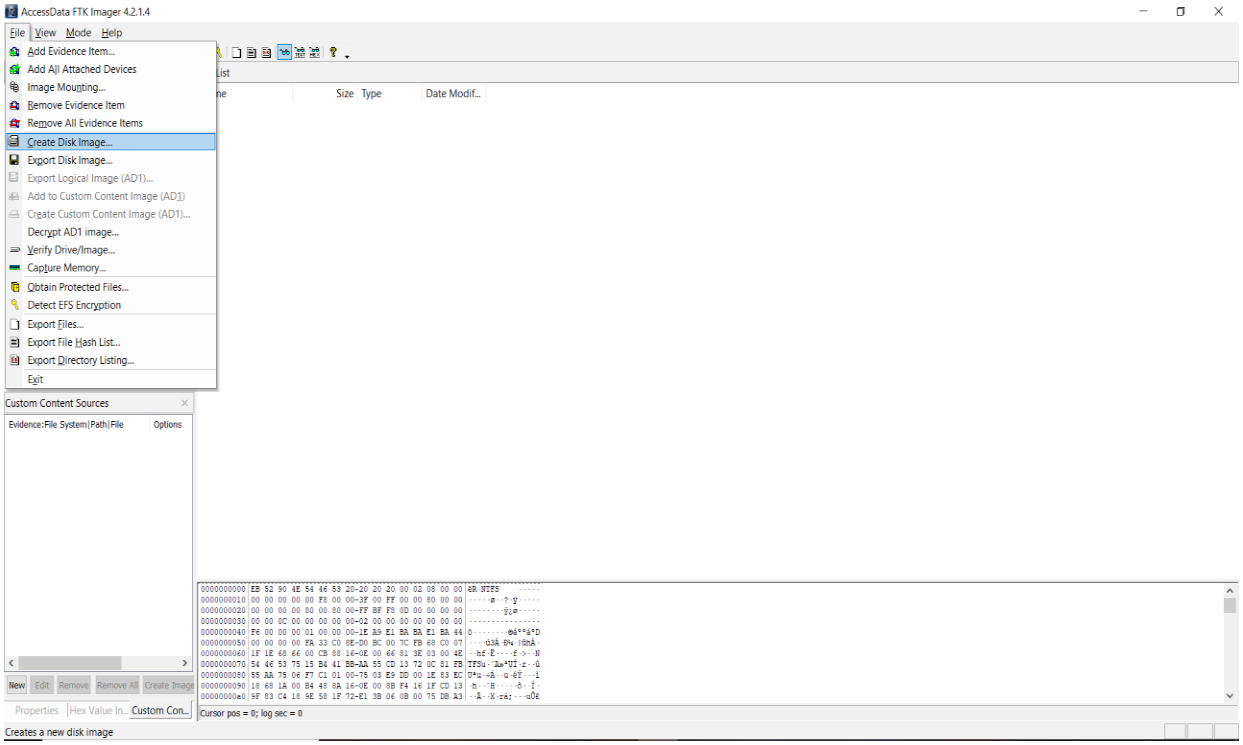
Please select from the following available drives:

C:\ - Windows [NTFS]

C:\ - Windows [NTFS]
D:\ - New Volume [NTFS]
E:\ - Case_SSD [NTFS]

Figure 31: Select the appropriate source drive.

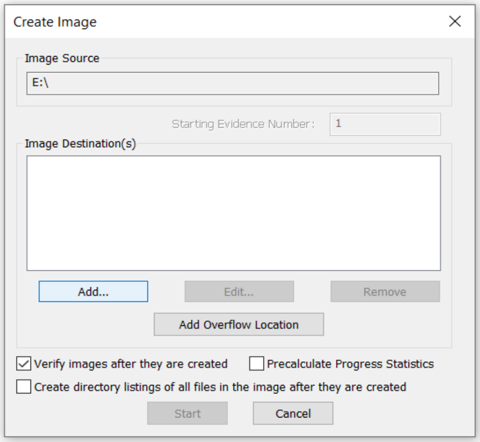
From figure 31, the source drive should be selected correctly. For example, from the above figure, if drive “D:\ New Volume” is selected instead of “F:\ Case_SSD,” the investigator ends up wasting a lot of time creating the image of a wrong data source drive. So always select the right source drive for creating an image. Then click on Finish. In the next step, go to File and Click on Create Disk Image, as shown in figure 32. This is the first step after the evidence is added to the FTK Imager tool. Then pops us a Dialogue box, as shown in figure 33. This dialogue box asks for the destination image type before that click on Add, and that will redirect to another dialogue box where destination image type is selected.



```
0000000000 EB 52 90 4E 54 46 53 20-20 20 20 00 02 08 00 00 ëR·NTFS    ·····
0000000010 00 00 00 00 00 F8 00 00-3F 00 FF 00 00 80 00 00 ·····ø··?·ÿ·····
0000000020 00 00 00 00 80 00 80 00-FF BF F8 0D 00 00 00 00 ········ÿ¿ø·····
0000000030 00 00 0C 00 00 00 00 00-02 00 00 00 00 00 00 00 ················
0000000040 F6 00 00 00 01 00 00 00-1E A9 E1 BA BA E1 BA 44 ö·······©á°°á°D
0000000050 00 00 00 00 FA 33 C0 8E-D0 BC 00 7C FB 68 C0 07 ····ú3À·Ð¼·|ûhÀ·
0000000060 1F 1E 68 66 00 CB 88 16-0E 00 66 81 3E 03 00 4E ··hf·Ë····f·>··N
0000000070 54 46 53 75 15 B4 41 BB-AA 55 CD 13 72 0C 81 FB TFSu·´A»ªUÍ·r··û
0000000080 55 AA 75 06 F7 C1 01 00-75 03 E9 DD 00 1E 83 EC Uªu·÷Á··u·éÝ···ì
0000000090 18 68 1A 00 B4 48 8A 16-0E 00 8B F4 16 1F CD 13 ·h··´H·····ô··Í·
00000000a0 9F 83 C4 18 9E 58 1F 72-E1 3B 06 0B 00 75 DB A3 ··Ä··X·rá;···uÛ£
```

Cursor pos = 0; log sec = 0

Figure 32: Create Disk Image.



Create Image

Image Source

E:\

Starting Evidence Number: 1

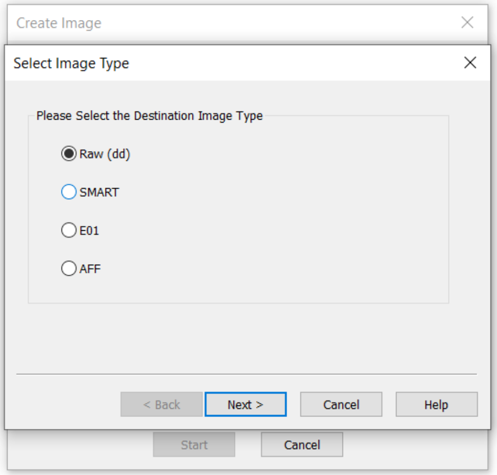
Image Destination(s)

☑ Verify images after they are created ☐ Precalculate Progress Statistics

☐ Create directory listings of all files in the image after they are created

Figure 33: Dialogue box for adding options before Image creation.

In the above figure 33, after adding the destination image type as “Raw (dd)” data dump, there are three checkboxes. These are optional. If the image created needs to be verified using MD5/SHA algorithms, then select the verify image checkbox. To display the time taken for image creation, select the Precalculate Progress Statistics checkbox.



Create Image

Select Image Type

Please Select the Destination Image Type

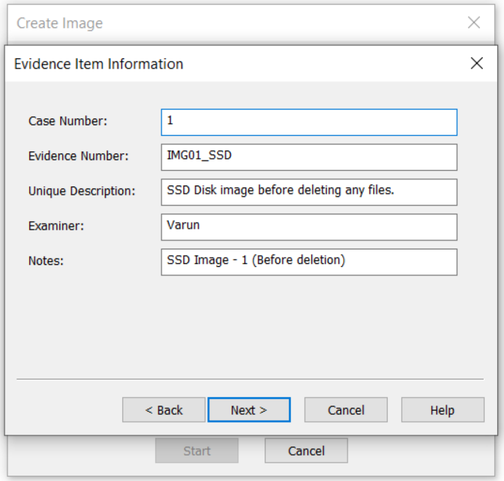
● Raw (dd)

○ SMART

○ E01

○ AFF

Figure 34: Selecting the destination image type.



Case Number: 1

Evidence Number: IMG01_SSD

Unique Description: SSD Disk image before deleting any files.

Examiner: Varun

Notes: SSD Image - 1 (Before deletion)

Figure 35: Image information for SSD.

Additional information about the SSD image being created is entered, as shown in figure 35. Name of the examiner conducting the investigation, case number, evidence number, unique description acts as a reference to the investigator. After entering all the information, click on Next.

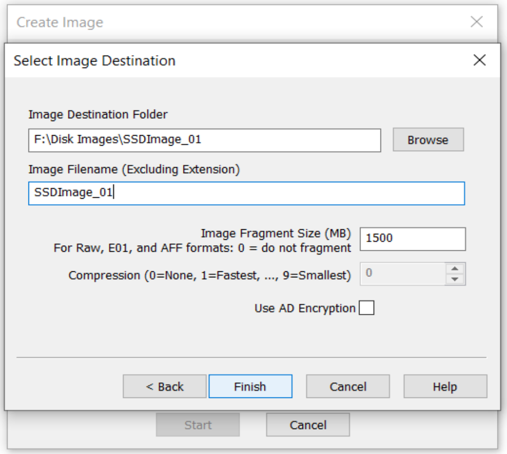


Image Destination Folder: F:\Disk Images\SSDImage_01

Image Filename (Excluding Extension): SSDImage_01

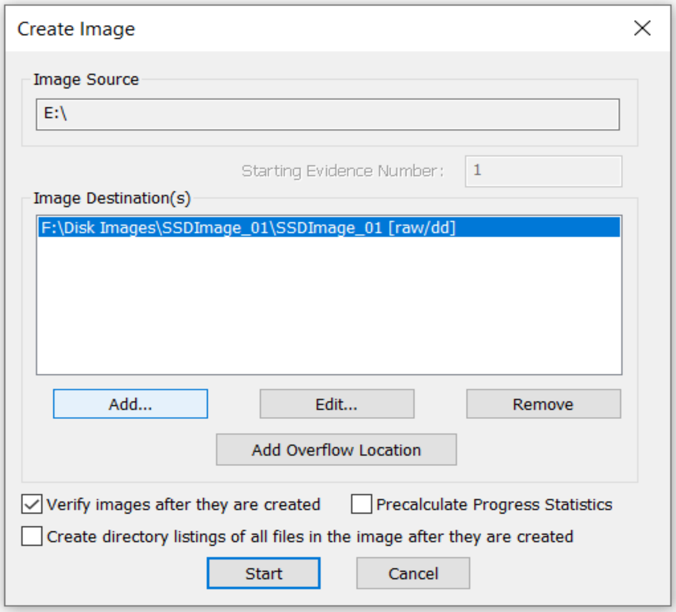
Image Fragment Size (MB)
For Raw, E01, and AFF formats: 0 = do not fragment: 1500

Compression (0=None, 1=Fastest, ..., 9=Smallest): 0

Use AD Encryption □

Figure 36: Destination image folder and file name.

In the above figure, the destination SSD image name and path of the file where it has to be stored is declared. As the created image size exceeds the storage in the investigator's laptop, an additional 4 TB hard drive (“Drive F:\”) is used. Image fragment size is given as 1500 MB. This makes the image file easier to handle when loaded to other tools for analysis. Click on the checkbox below compression to use AD encryption. This adds security to the image file created. As selecting this may take more time, here it is de-selected.



Create Image

Image Source: E:\

Starting Evidence Number: 1

Image Destination(s): F:\Disk Images\SSDImage_01\SSDImage_01 [raw/dd]

☑ Verify images after they are created

□ Precalculate Progress Statistics

□ Create directory listings of all files in the image after they are created

Figure 37: Dialogue box before starting image.

After adding the image destination in figure 37, click on start. All the steps so far were entering the right as required and selecting the source, destination image file paths. Below, figure 38 shows the progress of the image being created, and after image creating is 100%, image verification starts. After the image verification progress bar hits 100%, that means the image is created and verified to see if there is any data loss.

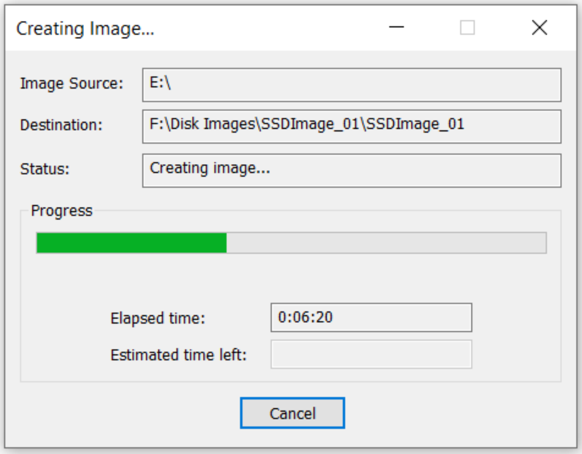


Image Source: E:\

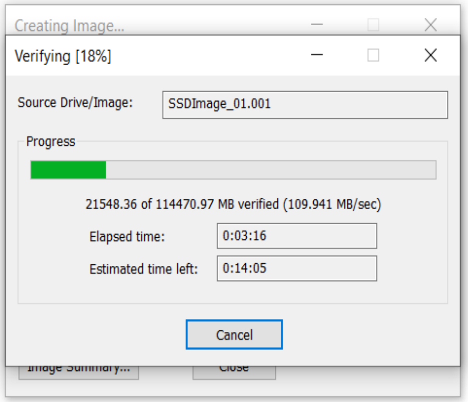
Destination: F:\Disk Images\SSDImage_01\SSDImage_01

Status: Creating image...

Elapsed time: 0:06:20

Estimated time left:

Figure 38: Image creation progress.



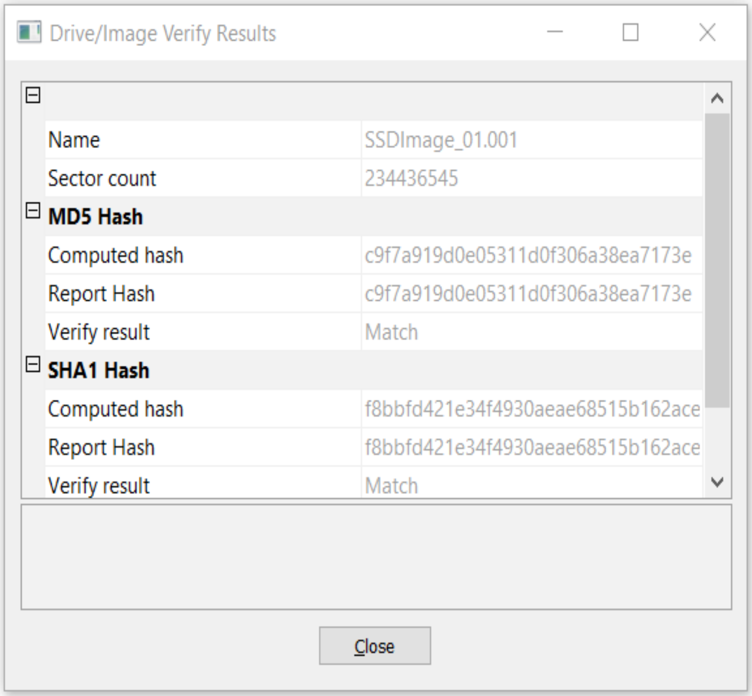
Source Drive/Image: SSDImage_01.001

21548.36 of 114470.97 MB verified (109.941 MB/sec)

Elapsed time: 0:03:16

Estimated time left: 0:14:05

Figure 39: Image verification progress.

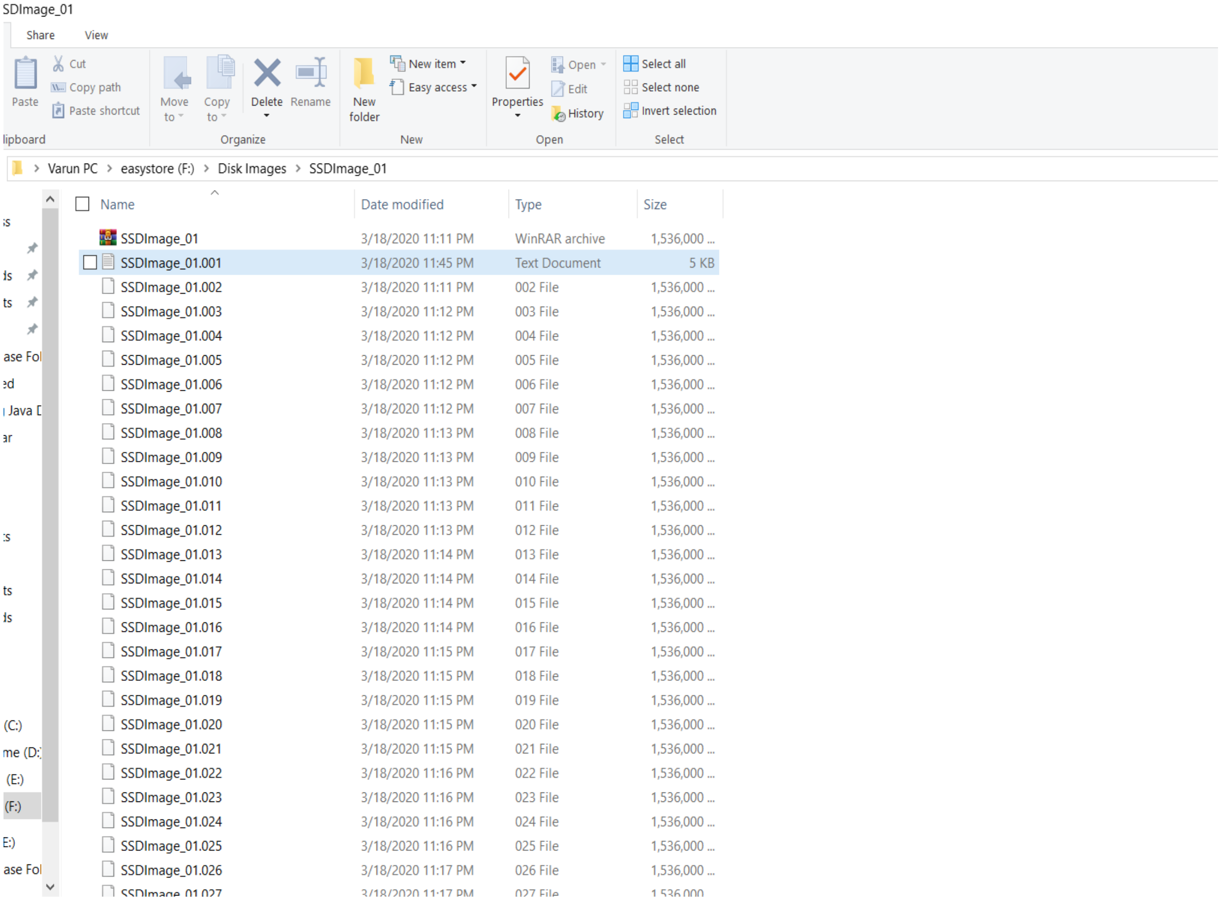


Drive/Image Verify Results

Name	SSDImage_01.001
Sector count	234436545
MD5 Hash	
Computed hash	c9f7a919d0e05311d0f306a38ea7173e
Report Hash	c9f7a919d0e05311d0f306a38ea7173e
Verify result	Match
SHA1 Hash	
Computed hash	f8bbfd421e34f4930aeae68515b162ace
Report Hash	f8bbfd421e34f4930aeae68515b162ace
Verify result	Match

Figure 40: Verified image results of SSD image 1.

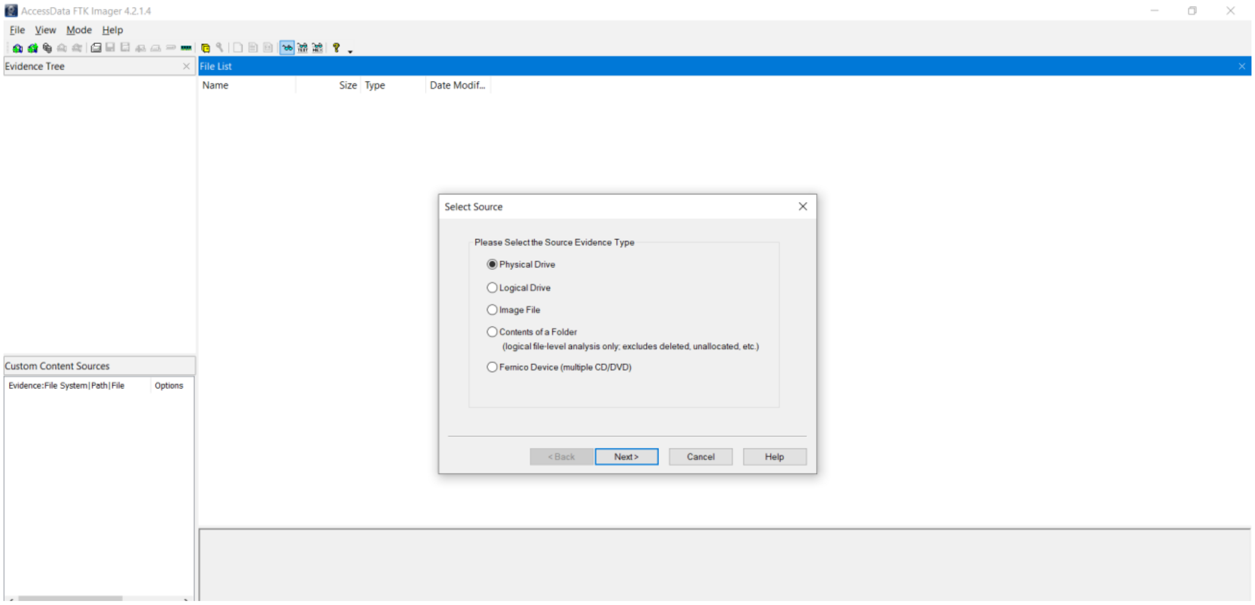
The hash values generate from MD5 and SHA 1 hashing algorithms after verification provides the result as matched. This verification is done by an investigator to make the evidence is not altered when subjected to different forensic tools for image creation. Figure 41 shows the final created image of SSD before deleting any files.



Name	Date modified	Type	Size
SSDImage_01	3/18/2020 11:11 PM	WinRAR archive	1,536,000 ...
SSDImage_01.001	3/18/2020 11:45 PM	Text Document	5 KB
SSDImage_01.002	3/18/2020 11:11 PM	002 File	1,536,000 ...
SSDImage_01.003	3/18/2020 11:12 PM	003 File	1,536,000 ...
SSDImage_01.004	3/18/2020 11:12 PM	004 File	1,536,000 ...
SSDImage_01.005	3/18/2020 11:12 PM	005 File	1,536,000 ...
SSDImage_01.006	3/18/2020 11:12 PM	006 File	1,536,000 ...
SSDImage_01.007	3/18/2020 11:12 PM	007 File	1,536,000 ...
SSDImage_01.008	3/18/2020 11:13 PM	008 File	1,536,000 ...
SSDImage_01.009	3/18/2020 11:13 PM	009 File	1,536,000 ...
SSDImage_01.010	3/18/2020 11:13 PM	010 File	1,536,000 ...
SSDImage_01.011	3/18/2020 11:13 PM	011 File	1,536,000 ...
SSDImage_01.012	3/18/2020 11:13 PM	012 File	1,536,000 ...
SSDImage_01.013	3/18/2020 11:14 PM	013 File	1,536,000 ...
SSDImage_01.014	3/18/2020 11:14 PM	014 File	1,536,000 ...
SSDImage_01.015	3/18/2020 11:14 PM	015 File	1,536,000 ...
SSDImage_01.016	3/18/2020 11:14 PM	016 File	1,536,000 ...
SSDImage_01.017	3/18/2020 11:15 PM	017 File	1,536,000 ...
SSDImage_01.018	3/18/2020 11:15 PM	018 File	1,536,000 ...
SSDImage_01.019	3/18/2020 11:15 PM	019 File	1,536,000 ...
SSDImage_01.020	3/18/2020 11:15 PM	020 File	1,536,000 ...
SSDImage_01.021	3/18/2020 11:15 PM	021 File	1,536,000 ...
SSDImage_01.022	3/18/2020 11:16 PM	022 File	1,536,000 ...
SSDImage_01.023	3/18/2020 11:16 PM	023 File	1,536,000 ...
SSDImage_01.024	3/18/2020 11:16 PM	024 File	1,536,000 ...
SSDImage_01.025	3/18/2020 11:16 PM	025 File	1,536,000 ...
SSDImage_01.026	3/18/2020 11:17 PM	026 File	1,536,000 ...
SSDImage_01.027	3/18/2020 11:17 PM	027 File	1,536,000

Figure 41: SSD Image file created using FTK Imager.

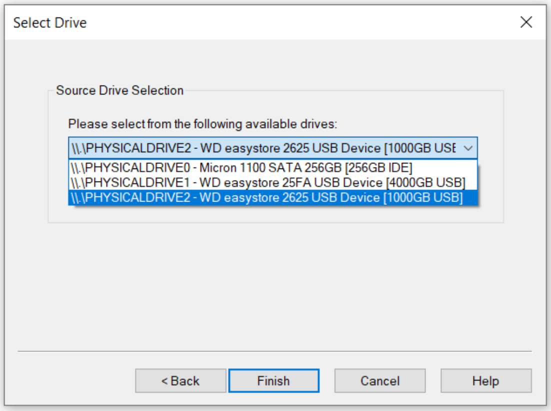
As the SSD image is extracted, it now starts the image creation for HDD. This is pretty much similar to the steps involved in creating an SSD image. All the important steps are captured and represented in the figures below. In the figure as step 1, select physical drive as HDD has physical moving parts to read/write data.



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.)
○ Femico Device (multiple CD/DVD)

Figure 42: Selecting source drive type.



Source Drive Selection

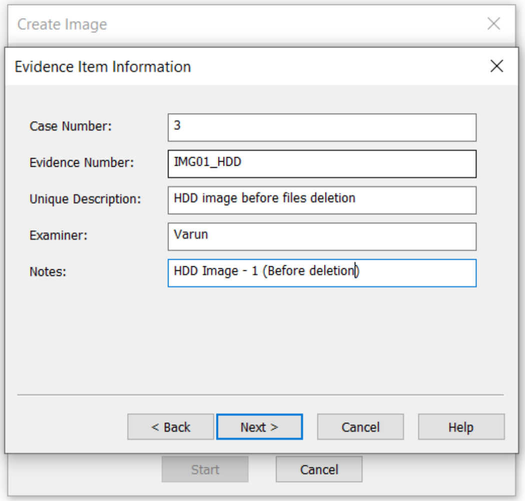
Please select from the following available drives:

\\.\PHYSICALDRIVE2 - WD easystore 2625 USB Device [1000GB USE
\\.\PHYSICALDRIVE0 - Micron 1100 SATA 256GB [256GB IDE]
\\.\PHYSICALDRIVE1 - WD easystore 25FA USB Device [4000GB USB]
\\.\PHYSICALDRIVE2 - WD easystore 2625 USB Device [1000GB USB]

Figure 43: Selecting the appropriate source drive (HDD).

After clicking on Finish, Add the destination image folder path and select the destination image type as Raw (dd) format. Type in all the image information, as shown in the figure below.

Then click on next for the dialogue box to be appeared asking for selecting the destination image path and click on start to begin the process of creating the HDD image.



Case Number: 3

Evidence Number: IMG01_HDD

Unique Description: HDD image before files deletion

Examiner: Varun

Notes: HDD Image - 1 (Before deletion)

Figure 44: Additional drive information.

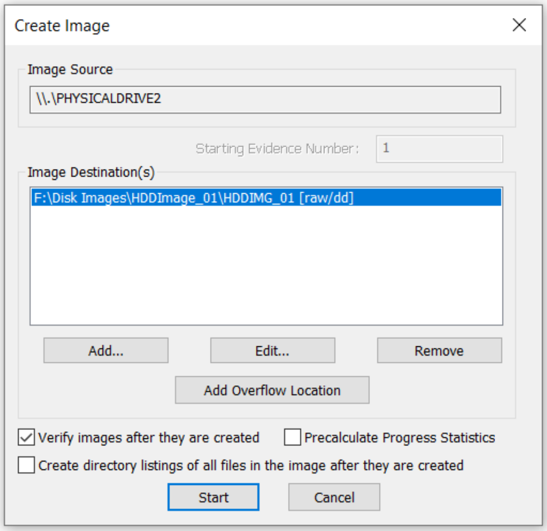


Image Source: \\.\PHYSICALDRIVE2

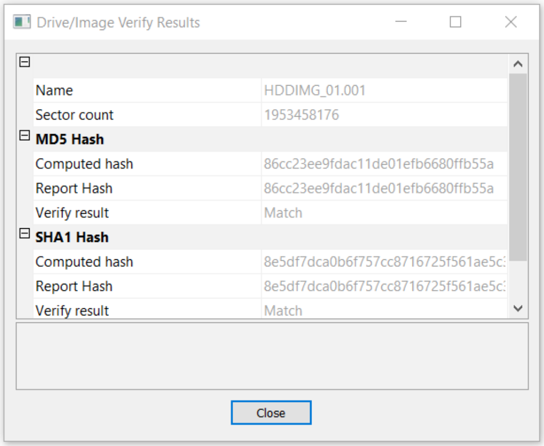
Starting Evidence Number: 1

Image Destination(s): F:\Disk Images\HDDImage_01\HDDIMG_01 [raw/dd]

☑ Verify images after they are created ☐ Precalculate Progress Statistics

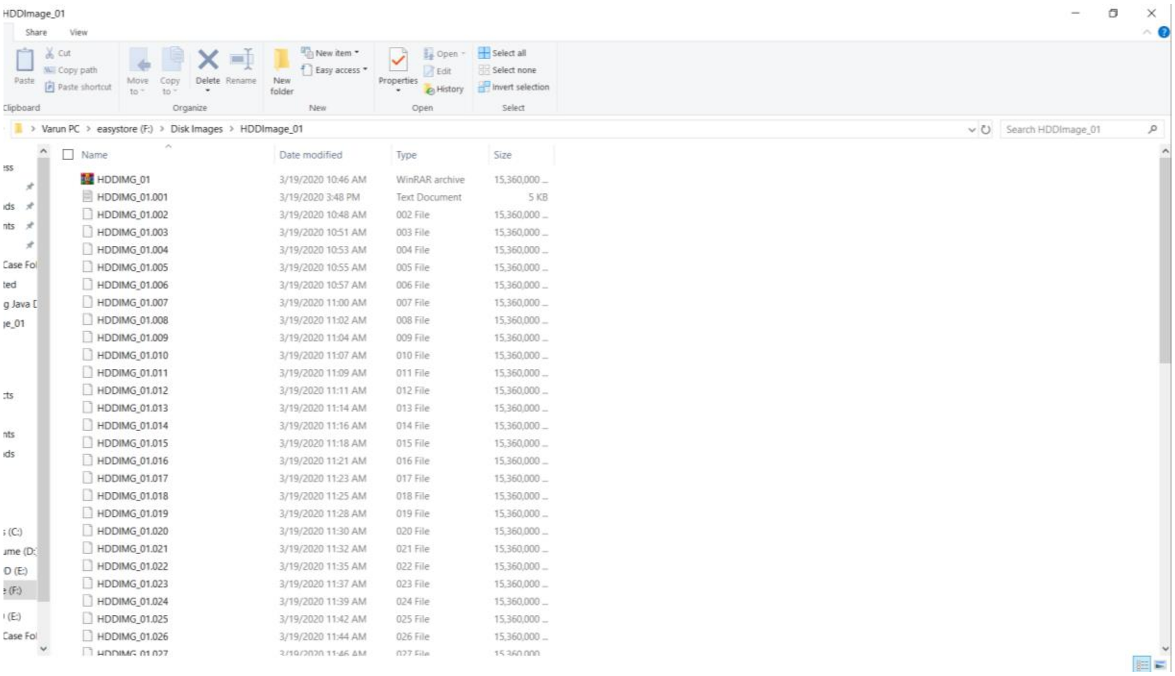
☐ Create directory listings of all files in the image after they are created

Figure 45: Dialogue box before starting image creation.



Name	HDDIMG_01.001
Sector count	1953458176
MD5 Hash	
Computed hash	86cc23ee9fdac11de01efb6680ffb55a
Report Hash	86cc23ee9fdac11de01efb6680ffb55a
Verify result	Match
SHA1 Hash	
Computed hash	8e5df7dca0b6f757cc8716725f561ae5c
Report Hash	8e5df7dca0b6f757cc8716725f561ae5c
Verify result	Match

Figure 46: Verified image results of HDD image 1.



Varun PC > easystore (F:) > Disk Images > HDDImage_01

Name	Date modified	Type	Size
HDDIMG_01	3/19/2020 10:46 AM	WinRAR archive	15,360,000 ...
HDDIMG_01.001	3/19/2020 3:48 PM	Text Document	5 KB
HDDIMG_01.002	3/19/2020 10:48 AM	002 File	15,360,000 ...
HDDIMG_01.003	3/19/2020 10:51 AM	003 File	15,360,000 ...
HDDIMG_01.004	3/19/2020 10:53 AM	004 File	15,360,000 ...
HDDIMG_01.005	3/19/2020 10:55 AM	005 File	15,360,000 ...
HDDIMG_01.006	3/19/2020 10:57 AM	006 File	15,360,000 ...
HDDIMG_01.007	3/19/2020 11:00 AM	007 File	15,360,000 ...
HDDIMG_01.008	3/19/2020 11:02 AM	008 File	15,360,000 ...
HDDIMG_01.009	3/19/2020 11:04 AM	009 File	15,360,000 ...
HDDIMG_01.010	3/19/2020 11:07 AM	010 File	15,360,000 ...
HDDIMG_01.011	3/19/2020 11:09 AM	011 File	15,360,000 ...
HDDIMG_01.012	3/19/2020 11:11 AM	012 File	15,360,000 ...
HDDIMG_01.013	3/19/2020 11:14 AM	013 File	15,360,000 ...
HDDIMG_01.014	3/19/2020 11:16 AM	014 File	15,360,000 ...
HDDIMG_01.015	3/19/2020 11:18 AM	015 File	15,360,000 ...
HDDIMG_01.016	3/19/2020 11:21 AM	016 File	15,360,000 ...
HDDIMG_01.017	3/19/2020 11:23 AM	017 File	15,360,000 ...
HDDIMG_01.018	3/19/2020 11:25 AM	018 File	15,360,000 ...
HDDIMG_01.019	3/19/2020 11:28 AM	019 File	15,360,000 ...
HDDIMG_01.020	3/19/2020 11:30 AM	020 File	15,360,000 ...
HDDIMG_01.021	3/19/2020 11:32 AM	021 File	15,360,000 ...
HDDIMG_01.022	3/19/2020 11:35 AM	022 File	15,360,000 ...
HDDIMG_01.023	3/19/2020 11:37 AM	023 File	15,360,000 ...
HDDIMG_01.024	3/19/2020 11:39 AM	024 File	15,360,000 ...
HDDIMG_01.025	3/19/2020 11:42 AM	025 File	15,360,000 ...
HDDIMG_01.026	3/19/2020 11:44 AM	026 File	15,360,000 ...
HDDIMG_01.027	3/19/2020 11:46 AM	027 File	15,360,000

Figure 47: HDD image file created using FTK Imager.

Figure 46 has the verified hash values after the image is completely created and verified. The final image file created is stored in external Hard drive as "HDDIMG_01," as shown in above figure 47.

Phase 2 - Extracting images from SSD and HDD (After Deleting evidence files):

After the images are created in phase 1, some evidence files related to the case scenario are deleted, and then another set of images is created. Below two figures show the selected evidence files, which will be deleted for further process in the study.

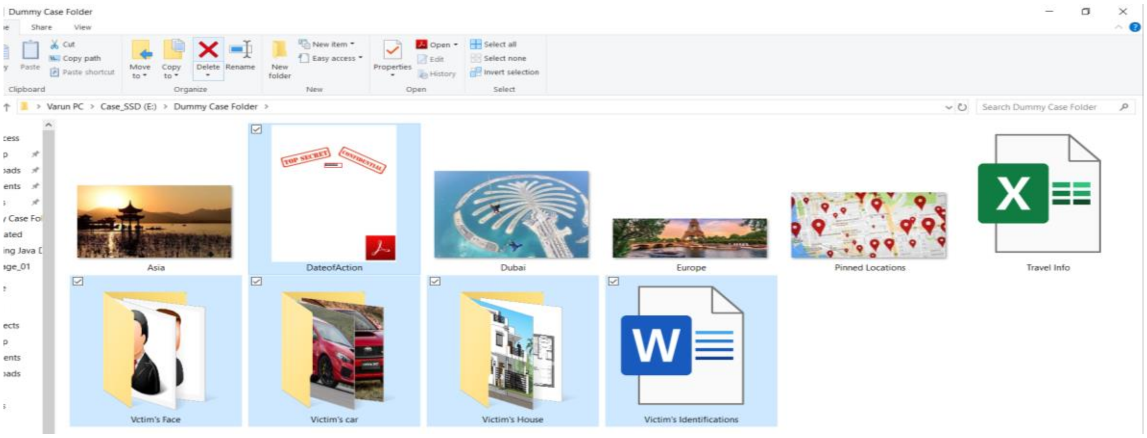


Figure 48: Files selected for deleting.

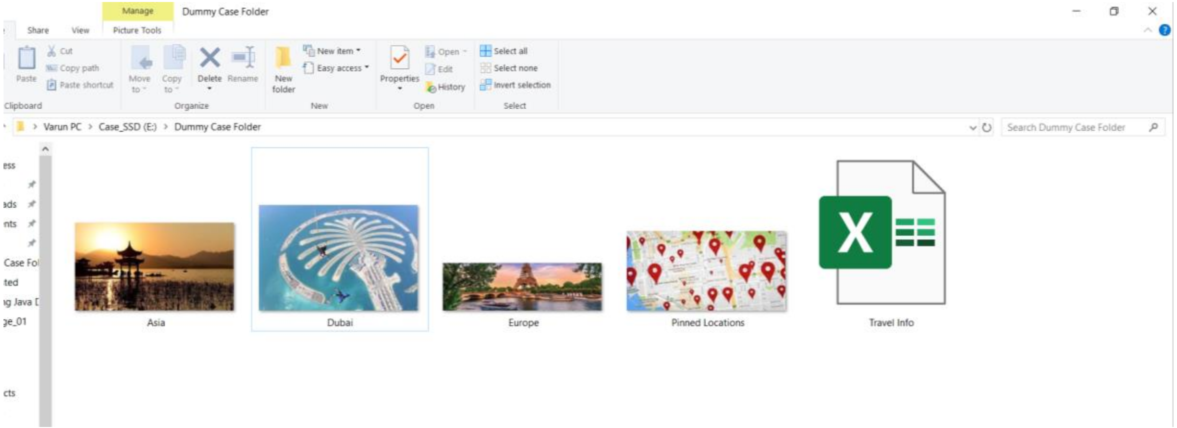
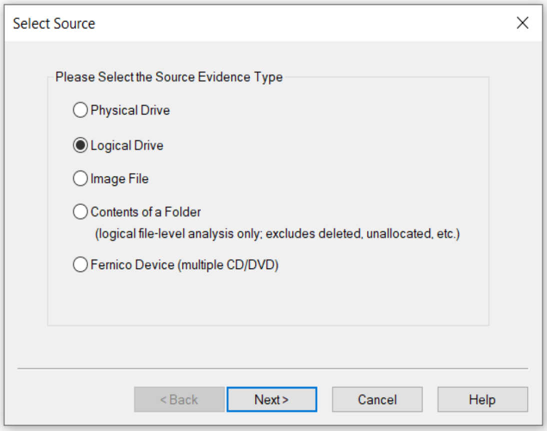


Figure 49: After deleting files in SSD.

Like phase 1, open FTK Imager for extracting images from SSD and HDD after deleting evidence files. Figures 50- figure 55 shows steps for SSD.



Select Source

Please Select the Source Evidence Type

○ Physical Drive

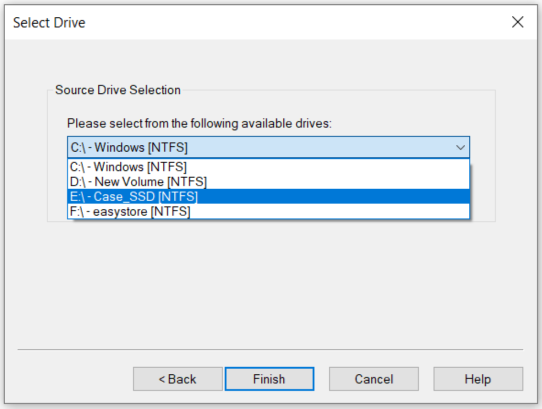
● Logical Drive

○ Image File

○ Contents of a Folder
(logical file-level analysis only; excludes deleted, unallocated, etc.)

○ Femico Device (multiple CD/DVD)

Figure 50: Selecting the source drive type.



Select Drive

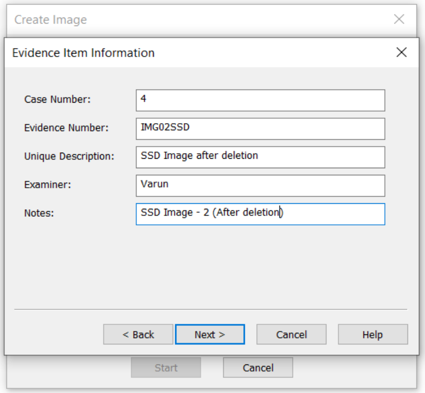
Source Drive Selection

Please select from the following available drives:

C:\ - Windows [NTFS]

C:\ - Windows [NTFS]
D:\ - New Volume [NTFS]
E:\ - Case_SSD [NTFS]
F:\ - easystore [NTFS]

Figure 51: Selecting the appropriate source drive.



Case Number: 4

Evidence Number: IMG02SSD

Unique Description: SSD Image after deletion

Examiner: Varun

Notes: SSD Image - 2 (After deletion)

Figure 52: Entering additional image information for SSD.

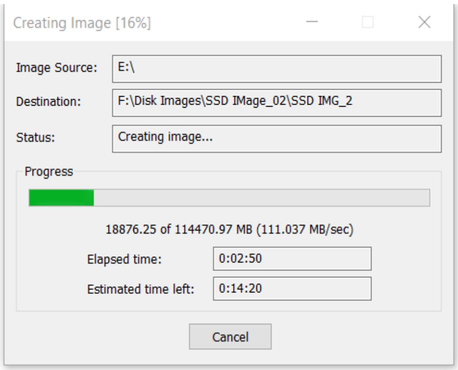


Image Source: E:\

Destination: F:\Disk Images\SSD IMage_02\SSD IMG_2

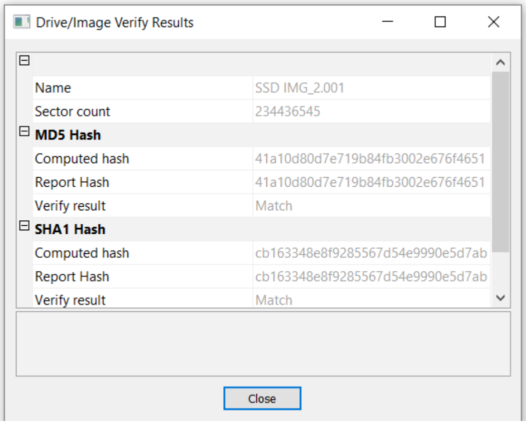
Status: Creating image...

18876.25 of 114470.97 MB (111.037 MB/sec)

Elapsed time: 0:02:50

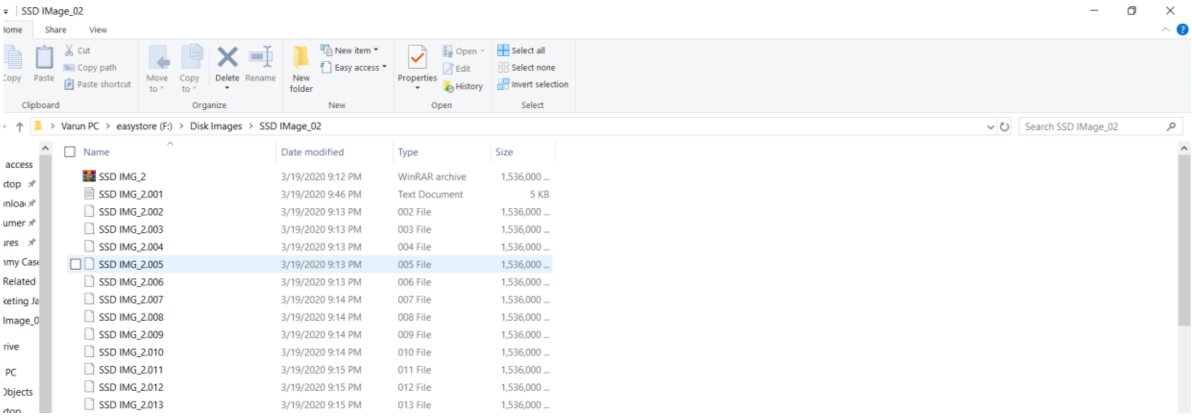
Estimated time left: 0:14:20

Figure 53: Image creation progress.



Name	SSD IMG_2.001
Sector count	234436545
MD5 Hash	
Computed hash	41a10d80d7e719b84fb3002e676f4651
Report Hash	41a10d80d7e719b84fb3002e676f4651
Verify result	Match
SHA1 Hash	
Computed hash	cb163348e8f9285567d54e9990e5d7ab
Report Hash	cb163348e8f9285567d54e9990e5d7ab
Verify result	Match

Figure 54: Verified image 2 results of SSD.



Name	Date modified	Type	Size
SSD IMG_2	3/19/2020 9:12 PM	WinRAR archive	1,536,000 ...
SSD IMG_2.001	3/19/2020 9:46 PM	Text Document	5 KB
SSD IMG_2.002	3/19/2020 9:13 PM	002 File	1,536,000 ...
SSD IMG_2.003	3/19/2020 9:13 PM	003 File	1,536,000 ...
SSD IMG_2.004	3/19/2020 9:13 PM	004 File	1,536,000 ...
SSD IMG_2.005	3/19/2020 9:13 PM	005 File	1,536,000 ...
SSD IMG_2.006	3/19/2020 9:13 PM	006 File	1,536,000 ...
SSD IMG_2.007	3/19/2020 9:14 PM	007 File	1,536,000 ...
SSD IMG_2.008	3/19/2020 9:14 PM	008 File	1,536,000 ...
SSD IMG_2.009	3/19/2020 9:14 PM	009 File	1,536,000 ...
SSD IMG_2.010	3/19/2020 9:14 PM	010 File	1,536,000 ...
SSD IMG_2.011	3/19/2020 9:15 PM	011 File	1,536,000 ...
SSD IMG_2.012	3/19/2020 9:15 PM	012 File	1,536,000 ...
SSD IMG_2.013	3/19/2020 9:15 PM	013 File	1,536,000 ...

Figure 55: Created image 2 of SSD.

Figure 55 shows “SSD IMG_2” is created and stored in an external hard drive, which will further be used for analysis. Similar steps are followed for HDD, starting from figure 56 below.

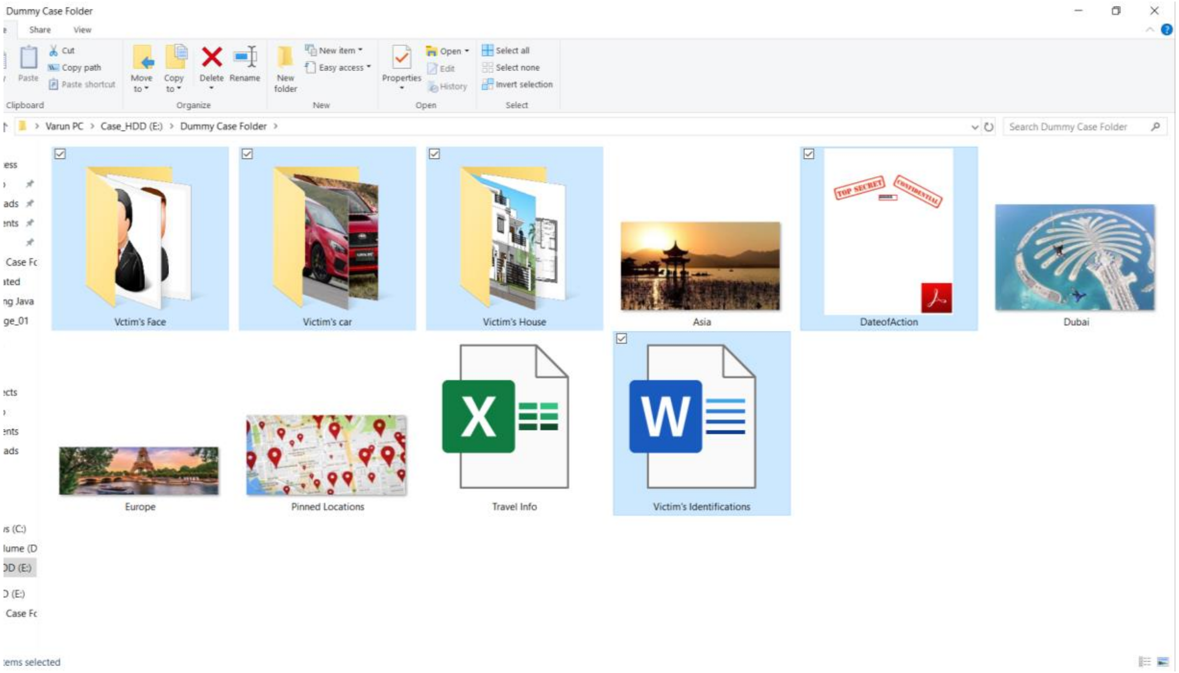


Figure 56: Evidence files selected for deleting.

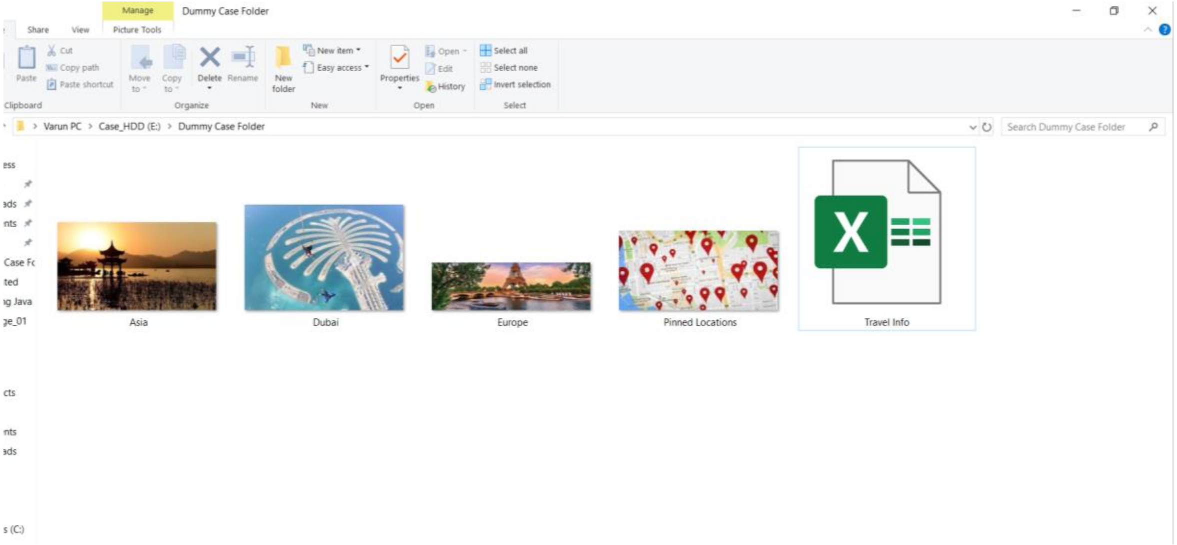
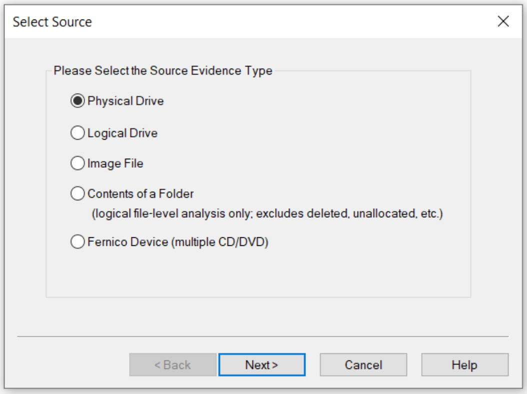


Figure 57: After deleting evidence files from HDD.

Once the evidence files related to the case are deleted from the HDD, this drive is subjected to FTK Imager for creating an image like SSD. The steps involving in this process are the same as above.


Select Source

Please Select the Source Evidence Type

● Physical Drive

○ Logical Drive

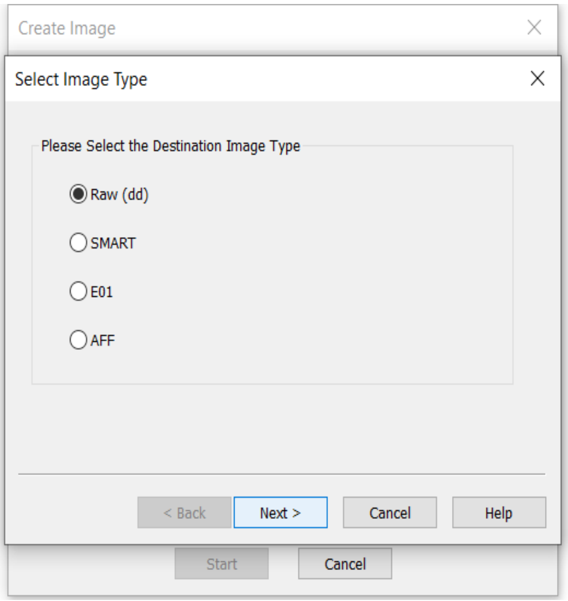
○ Image File

○ Contents of a Folder
(logical file-level analysis only; excludes deleted, unallocated, etc.)

○ Fernico Device (multiple CD/DVD)

< Back | Next > | Cancel | Help

Figure 58: Selecting source drive type for HDD.



Please Select the Destination Image Type

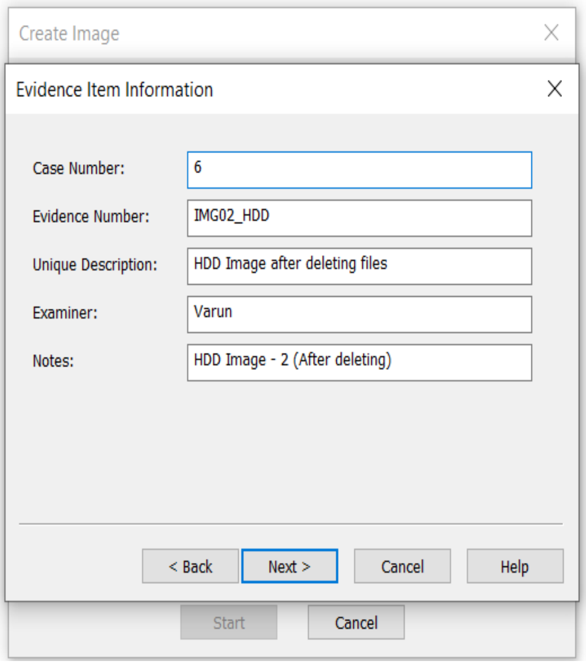
● Raw (dd)

○ SMART

○ E01

○ AFF

Figure 59: Selecting the destination image type.



Case Number: 6

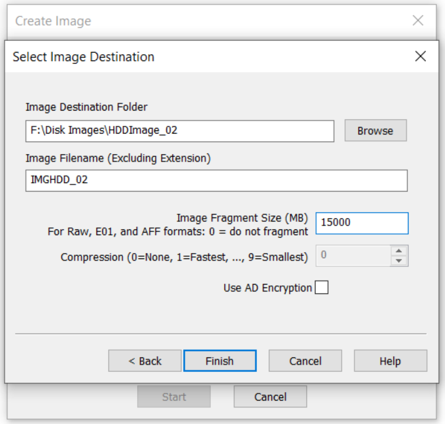
Evidence Number: IMG02_HDD

Unique Description: HDD Image after deleting files

Examiner: Varun

Notes: HDD Image - 2 (After deleting)

Figure 60: Enter the additional information for HDD image 2.



Create Image

Select Image Destination

Image Destination Folder: F:\Disk Images\HDDImage_02

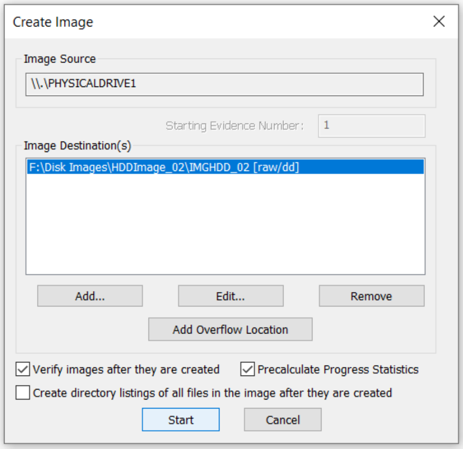
Image Filename (Excluding Extension): IMGHDD_02

Image Fragment Size (MB)
For Raw, E01, and AFF formats: 0 = do not fragment: 15000

Compression (0=None, 1=Fastest, ..., 9=Smallest): 0

Use AD Encryption □

Figure 61: Select image destination folder.



Create Image

Image Source: \\.\PHYSICALDRIVE1

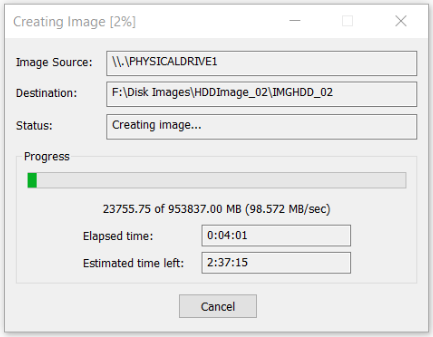
Starting Evidence Number: 1

Image Destination(s): F:\Disk Images\HDDImage_02\IMGHDD_02 [raw/dd]

☑ Verify images after they are created ☑ Precalculate Progress Statistics

□ Create directory listings of all files in the image after they are created

Figure 62: Click on start to create an image of HDD.



Creating Image [2%]

Image Source: \\.\PHYSICALDRIVE1

Destination: F:\Disk Images\HDDImage_02\IMGHDD_02

Status: Creating image...

Progress

23755.75 of 953837.00 MB (98.572 MB/sec)

Elapsed time: 0:04:01

Estimated time left: 2:37:15

Figure 63: Image creation progress.

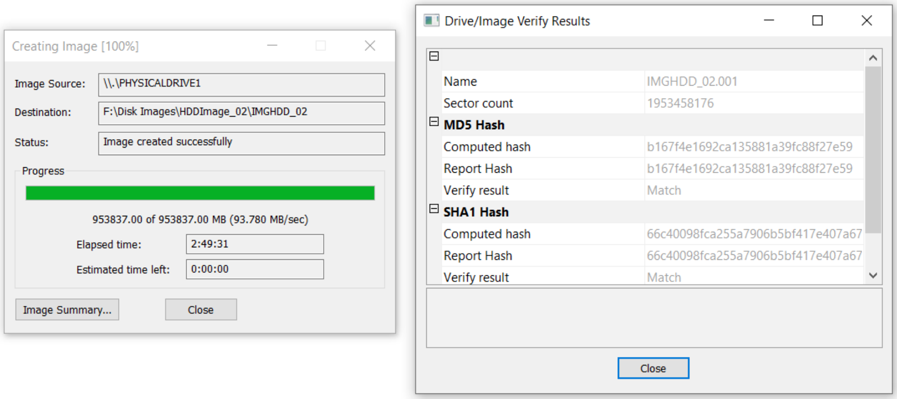
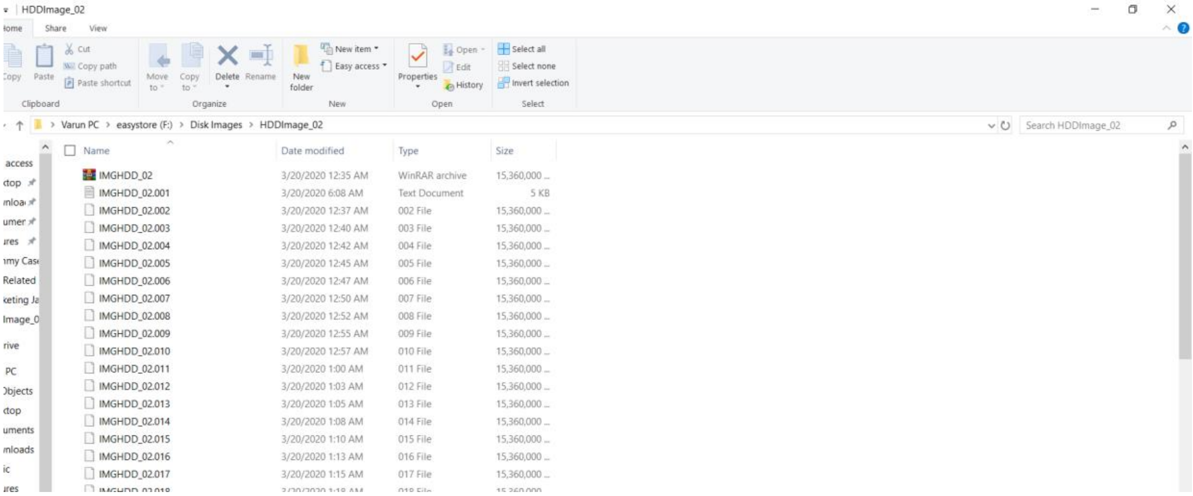


Image Source: \\.\PHYSICALDRIVE1
Destination: F:\Disk Images\HDDImage_02\IMGHDD_02
Status: Image created successfully

953837.00 of 953837.00 MB (93.780 MB/sec)
Elapsed time: 2:49:31
Estimated time left: 0:00:00

Name	IMGHDD_02.001
Sector count	1953458176
MD5 Hash	
Computed hash	b167f4e1692ca135881a39fc88f27e59
Report Hash	b167f4e1692ca135881a39fc88f27e59
Verify result	Match
SHA1 Hash	
Computed hash	66c40098fca255a7906b5bf417e407a67
Report Hash	66c40098fca255a7906b5bf417e407a67
Verify result	Match

Figure 64: Verified image results for HDD image 2.



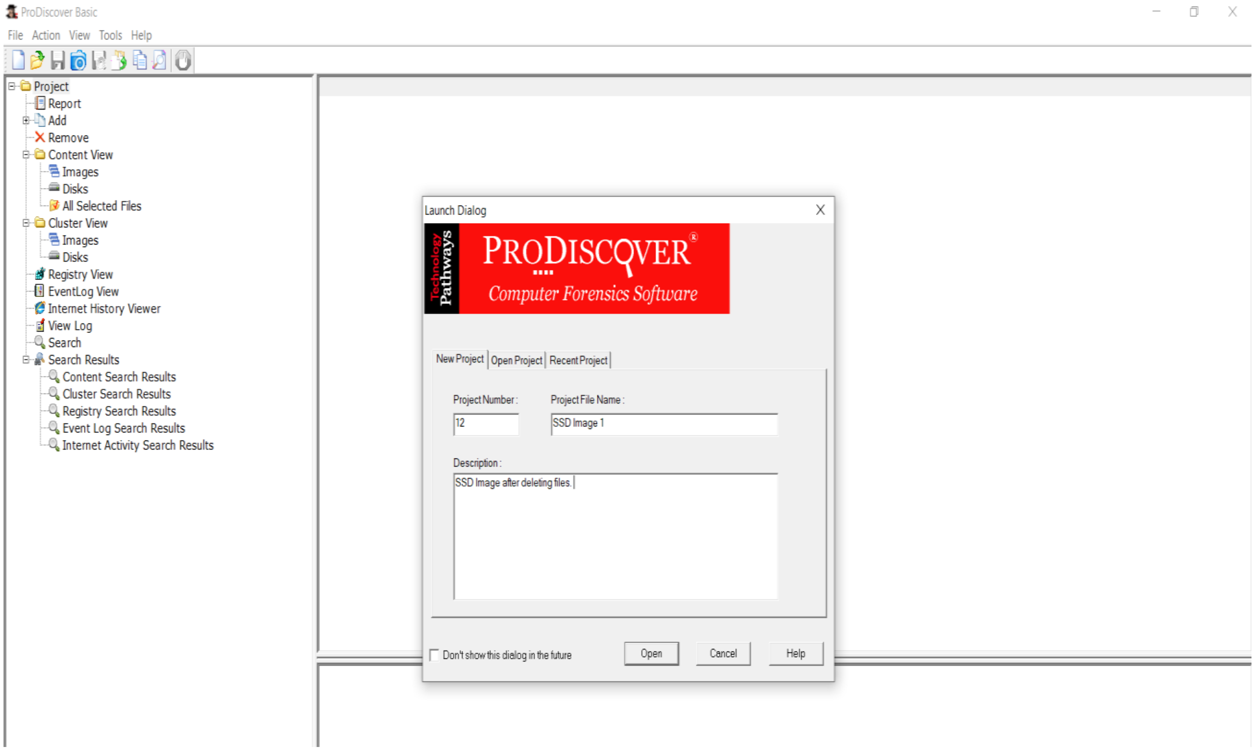
Name	Date modified	Type	Size
IMGHDD_02	3/20/2020 12:35 AM	WinRAR archive	15,360,000 ...
IMGHDD_02.001	3/20/2020 6:08 AM	Text Document	5 KB
IMGHDD_02.002	3/20/2020 12:37 AM	002 File	15,360,000 ...
IMGHDD_02.003	3/20/2020 12:40 AM	003 File	15,360,000 ...
IMGHDD_02.004	3/20/2020 12:42 AM	004 File	15,360,000 ...
IMGHDD_02.005	3/20/2020 12:45 AM	005 File	15,360,000 ...
IMGHDD_02.006	3/20/2020 12:47 AM	006 File	15,360,000 ...
IMGHDD_02.007	3/20/2020 12:50 AM	007 File	15,360,000 ...
IMGHDD_02.008	3/20/2020 12:52 AM	008 File	15,360,000 ...
IMGHDD_02.009	3/20/2020 12:55 AM	009 File	15,360,000 ...
IMGHDD_02.010	3/20/2020 12:57 AM	010 File	15,360,000 ...
IMGHDD_02.011	3/20/2020 1:00 AM	011 File	15,360,000 ...
IMGHDD_02.012	3/20/2020 1:03 AM	012 File	15,360,000 ...
IMGHDD_02.013	3/20/2020 1:05 AM	013 File	15,360,000 ...
IMGHDD_02.014	3/20/2020 1:08 AM	014 File	15,360,000 ...
IMGHDD_02.015	3/20/2020 1:10 AM	015 File	15,360,000 ...
IMGHDD_02.016	3/20/2020 1:13 AM	016 File	15,360,000 ...
IMGHDD_02.017	3/20/2020 1:15 AM	017 File	15,360,000 ...
IMGHDD_02.018	3/20/2020 1:18 AM	018 File	15,360,000

Figure 65: After creating HDD Image 2.

Now that all the 4 images are created from SSD drives, they are saved in the Disk images folder with names “HDDIMG_01”, “IMGHDD_02”, “SSDImage_01”, and “SSD IMG_2” as shown in figures. These images are loaded to Autopsy forensic tool to analyze the results obtained.

As ProDiscover Basic is another tool used in this study, the process of capturing an image is shown in the next figures. Since most of the research studies have proven that deleted images can be retrieved from HDD, this study concentrates on analyzing only SSD images.

Here, image for SSD before deleting any files haven't been captured as there will be no results obtained. Hence ProDiscover Basic here is used to create the image of SSD after deleting the evidence files. Start the ProDiscover Basic tool, click on New Project, and give the project a name, number, unique description as a reference for the investigator. Click on Open and then click on Action to capture the image of a drive, as shown in figure 67.



Project Number: 12

Project File Name: SSD Image 1

Description: SSD Image after deleting files.

☐ Don't show this dialog in the future

Figure 66: Creating a new project in ProDiscover Basic.

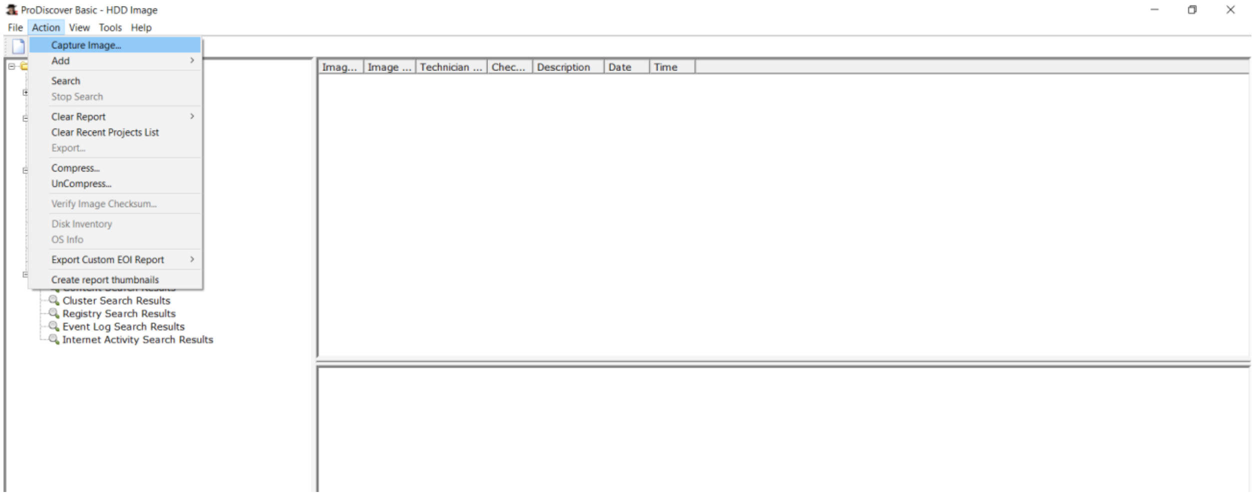
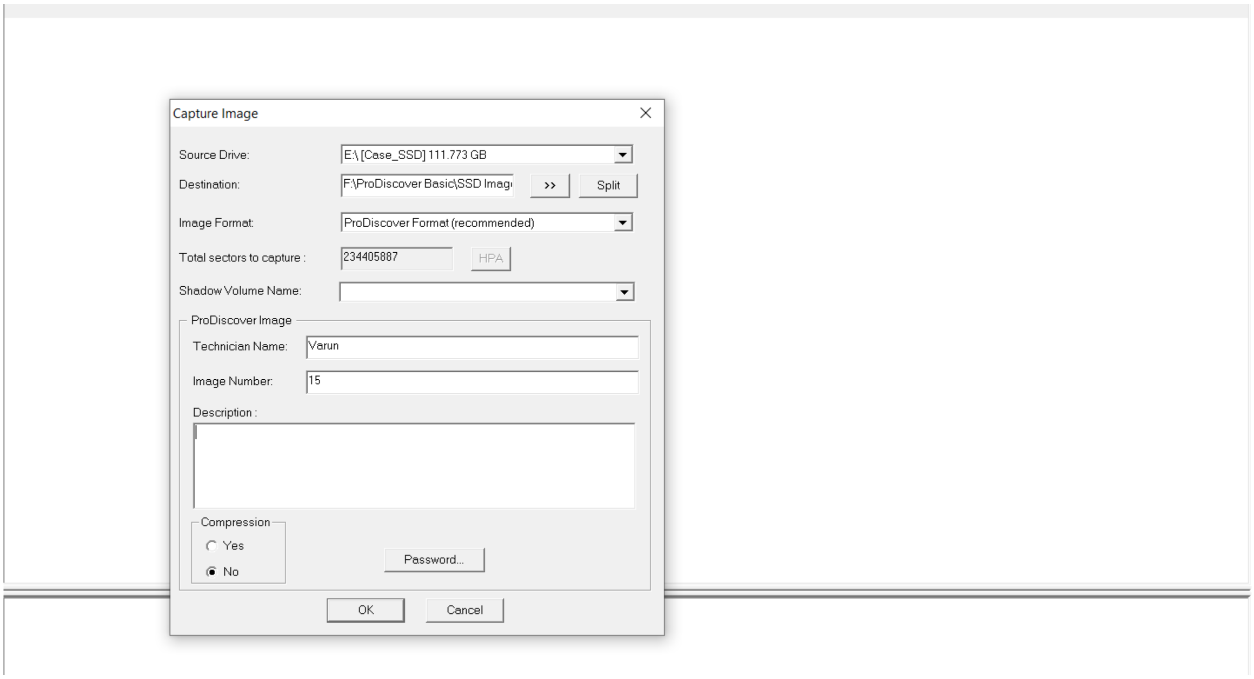


Figure 67: capturing an image using ProDiscover.



Capture Image

Source Drive: E:\ [Case_SSD] 111.773 GB

Destination: F:\ProDiscover Basic\SSD Imag

Image Format: ProDiscover Format (recommended)

Total sectors to capture : 234405887

Shadow Volume Name:

ProDiscover Image

Technician Name: Varun

Image Number: 15

Description :

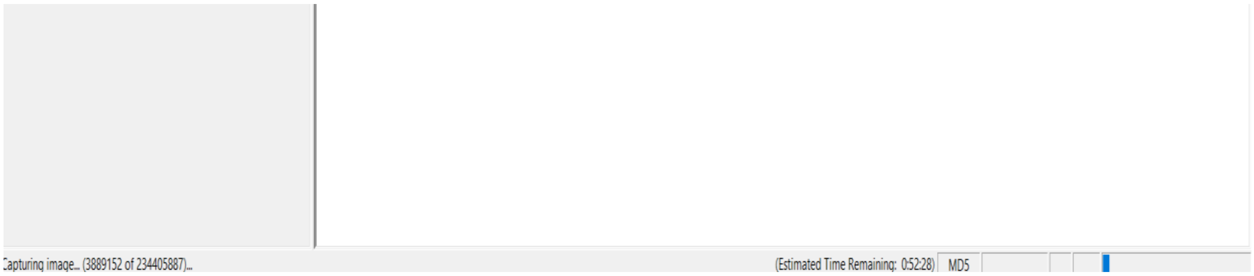
Compression

○ Yes

● No

Figure 68: Captured image details.

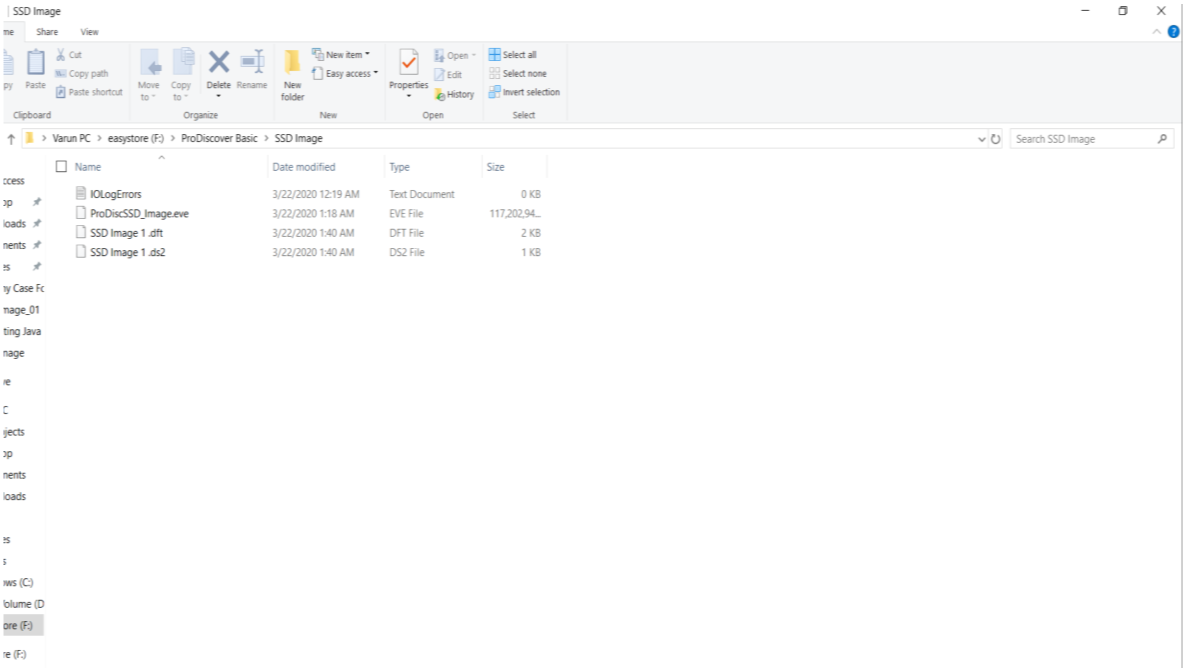
In the above Capture Image window, enter all the details of source image, image destination, image file name, image file type, examiner name, image reference number, and then click on “OK” to create the image of the disc. In the bottom left of the next figure, displayed is the progress of capturing the image. The displayed count number is sector count, i.e., the number of sectors captured out of total sectors the drive has. The estimated time remaining was displayed around 52 minutes for 120 GB SSD, whereas for 1 TB hard drive, it was around 26 hours. Once the image is created, it is saved as “ProDiscSSD_image.eve,” as shown in figure 70. This image will be added to the ProDiscover Basic tool to analyze and understand SSD's behavior.



Capturing image... (3889152 of 234405887)...

(Estimated Time Remaining: 0:52:28) MD5

Figure 69: Progress of the captured image.



SSD Image

Varun PC > easystore (F:) > ProDiscover Basic > SSD Image

Search SSD Image

Name	Date modified	Type	Size
IOLogErrors	3/22/2020 12:19 AM	Text Document	0 KB
ProDiscSSD_Image.eve	3/22/2020 1:18 AM	EVE File	117,202,94...
SSD Image 1 .dft	3/22/2020 1:40 AM	DFT File	2 KB
SSD Image 1 .ds2	3/22/2020 1:40 AM	DS2 File	1 KB

Figure 70: After the SSD image is created.

Data Analysis

After the data presentation has been successfully completed, i.e., step by step process of image extraction is clearly explained, the next section is data analysis. In this section, all the images created using FTK Imager will be analyzed using Autopsy, and an SSD image created using ProDiscover Basic will be analyzed by the same tool itself. Each figure and its content will be explained in detail below, and by the end of this section, the investigator observes results obtained from these tools, which then will be presented in the next chapter under the results section.

First, both the images created from SSD and HDD before deleting any evidence files i.e., image 1. These respective images will be analyzed, and reports will be generated. Like image 1, the same process is followed for images extracted from drives after deleting evidence data i.e. image 2. After all the reports generated by Autopsy, another report will be generated using ProDiscover Basic. Starting with the analysis of SSD image 1 below.

If this is this first-time Autopsy is loaded in the investigator's laptop, click on the new case, and add the SSD image created before deleting any evidence files. If an image is added and closed without exiting, then click on the open recent case when it is highlighted. It is disabled in the below figure, which means no case was recently opened. Figure 72 shows case information that needs to be entered. A case name, the base directory where the analyzed image results are stored. In this case, results are stored in “drive F:\Autopsy.” Then click on “Next.” A new case database and text index will be created with the case name provided.

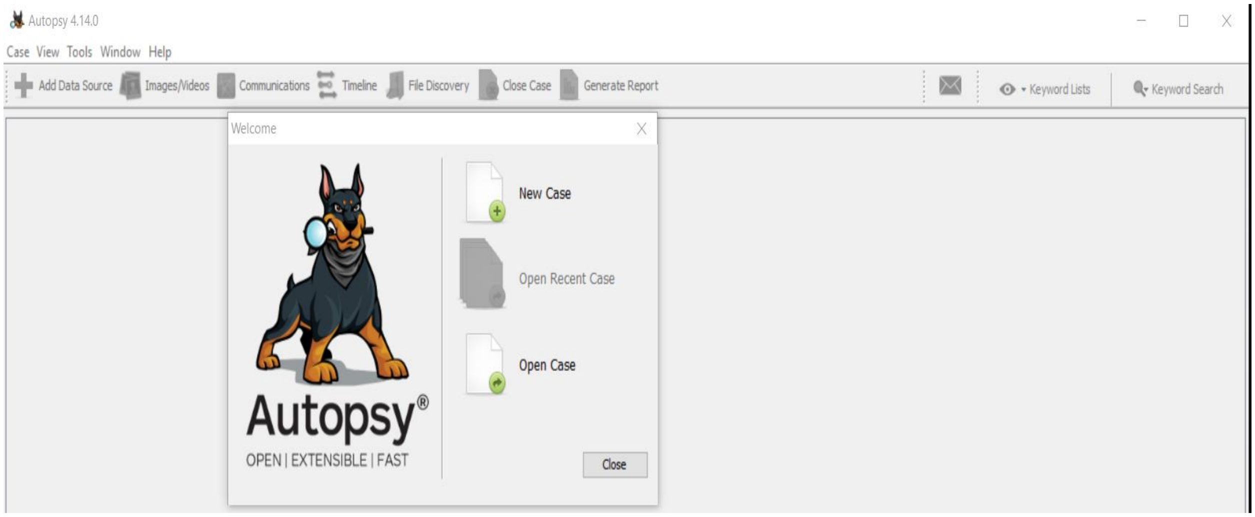
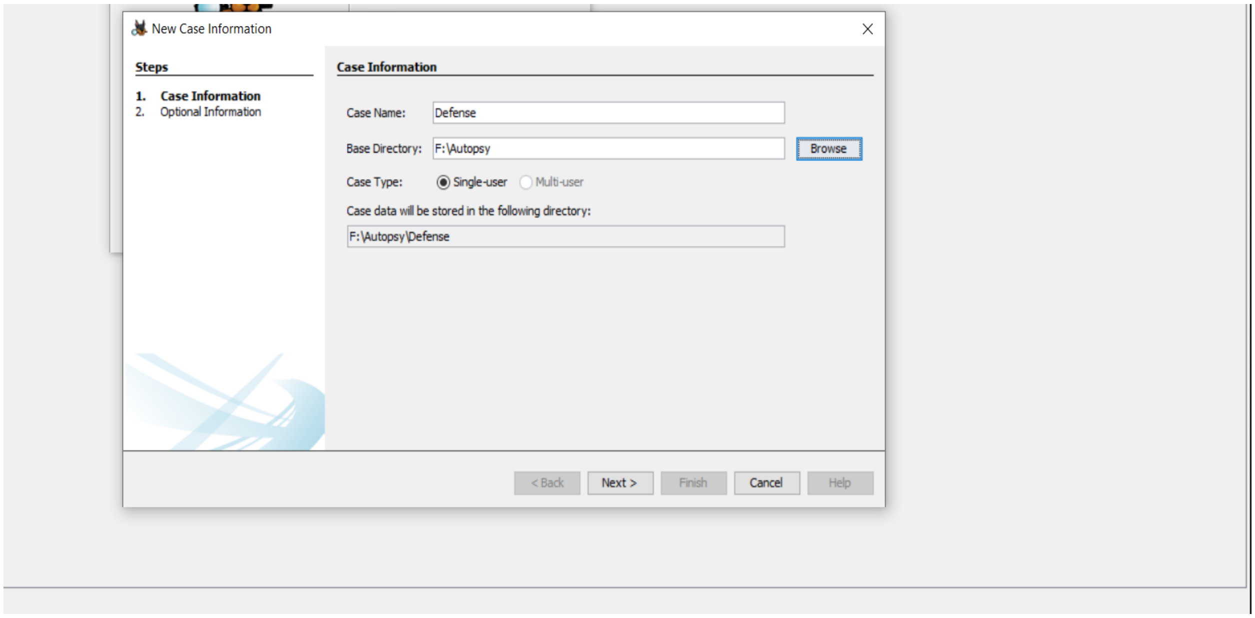


Figure 71: Start a new case in Autopsy.



Case Name: Defense

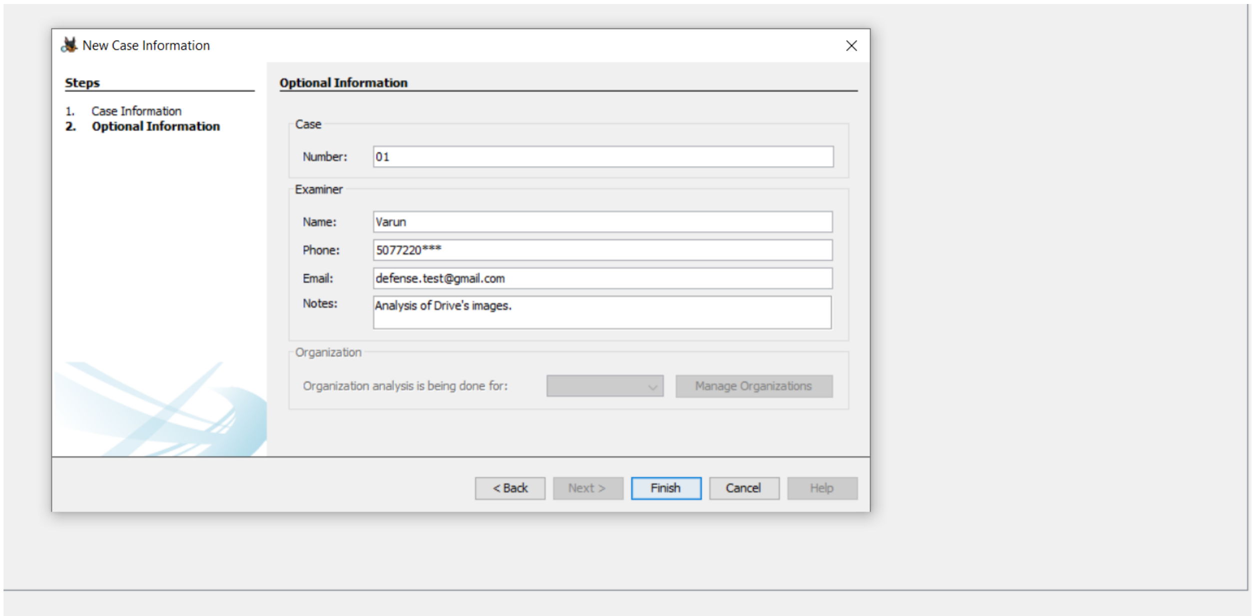
Base Directory: F:\Autopsy

Case Type: ● Single-user ○ Multi-user

Case data will be stored in the following directory:

F:\Autopsy\Defense

Figure 72: Enter case information.



New Case Information

Steps

1. Case Information
2. **Optional Information**

Optional Information

Case

Number: 01

Examiner

Name: Varun

Phone: 5077220***

Email: defense.test@gmail.com

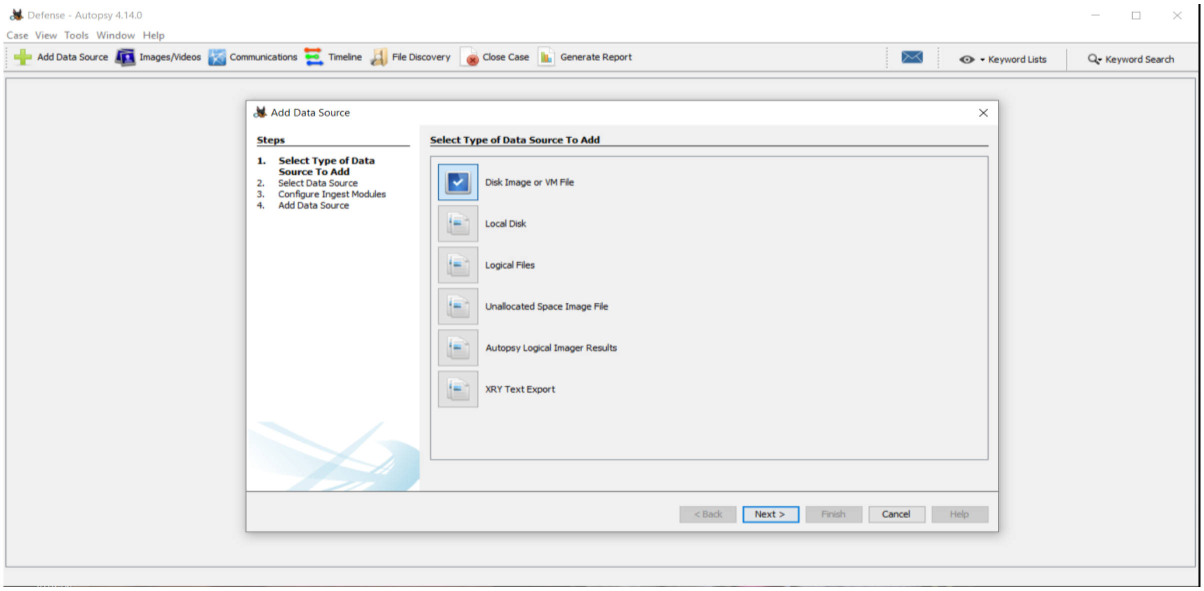
Notes: Analysis of Drive's images.

Organization

Organization analysis is being done for:

Figure 73: Enter optional SSD image information.

Additional information like a case number, examiner name, phone, email, and unique description is entered, as shown in figure 73. In the below figure, select the source data type as “Data Image” and click on Next.



Defense - Autopsy 4.14.0

Add Data Source

Steps

1. **Select Type of Data Source To Add**
2. Select Data Source
3. Configure Ingest Modules
4. Add Data Source

Select Type of Data Source To Add

☑ Disk Image or VM File

Local Disk

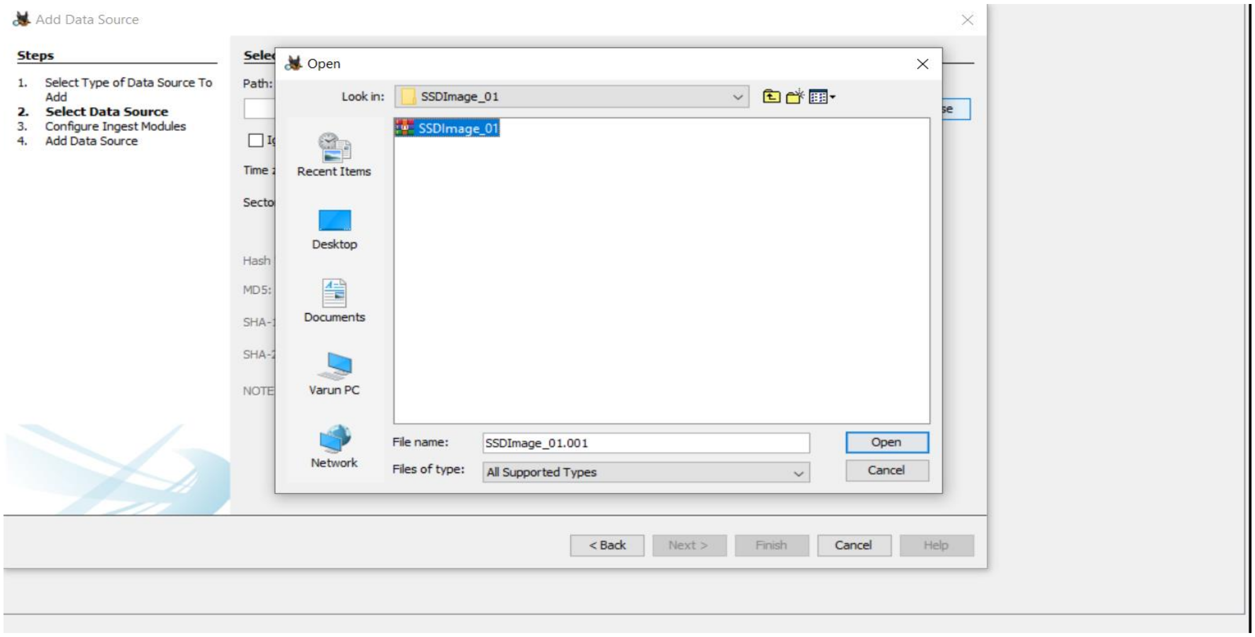
Logical Files

Unallocated Space Image File

Autopsy Logical Imager Results

XRY Text Export

Figure 74: Select the data source type to add.



Steps

1. Select Type of Data Source To Add
2. **Select Data Source**
3. Configure Ingest Modules
4. Add Data Source

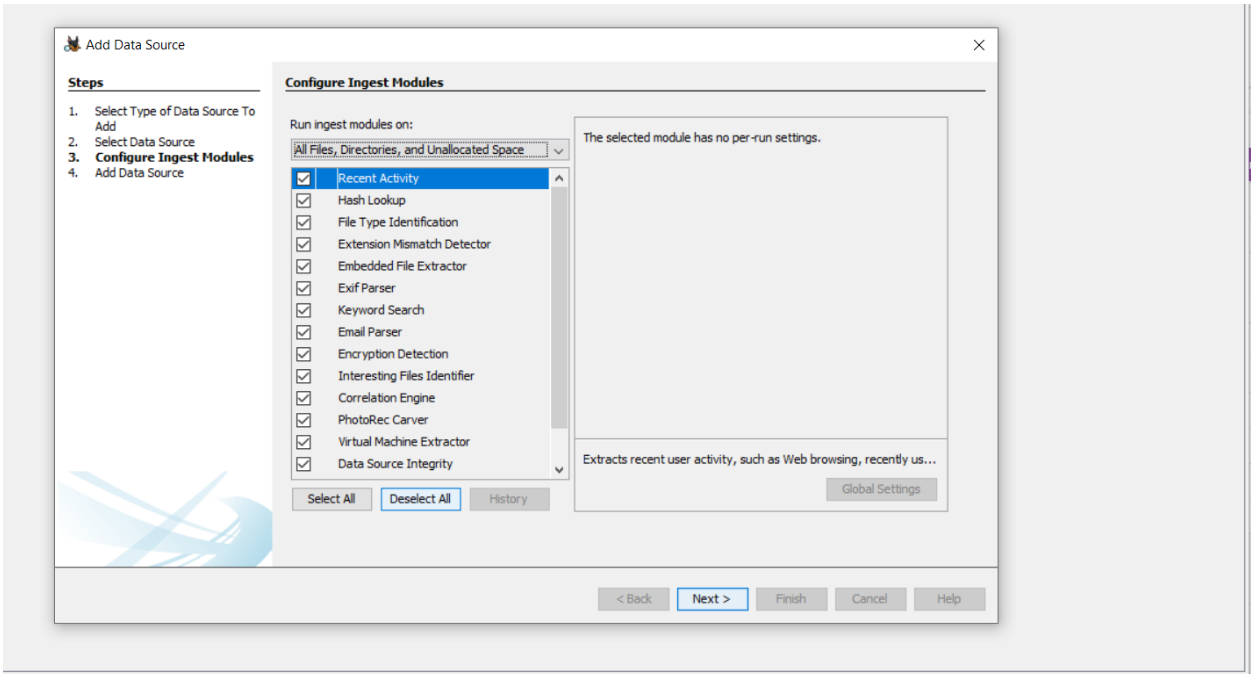
Look in: SSDImage_01

SSDImage_01

File name: SSDImage_01.001

Files of type: All Supported Types

Figure 75: Select source SSD image to open.



Steps

1. Select Type of Data Source To Add
2. Select Data Source
3. **Configure Ingest Modules**
4. Add Data Source

Configure Ingest Modules

Run ingest modules on: All Files, Directories, and Unallocated Space

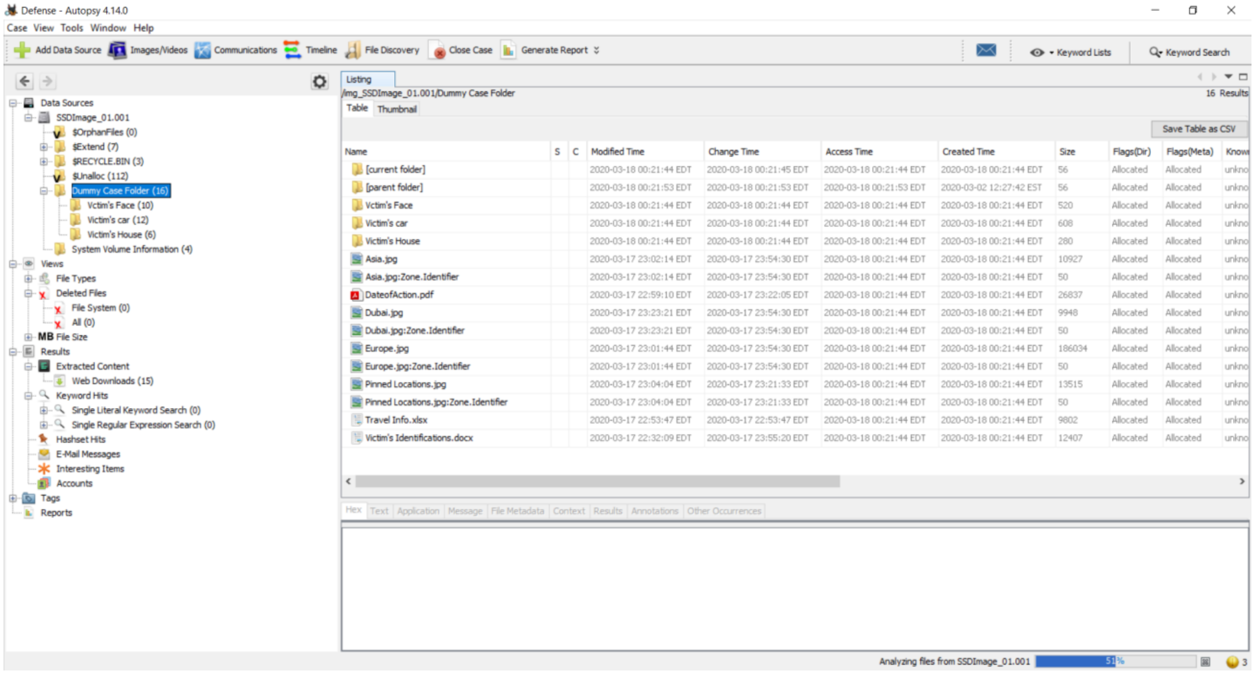
- ☑ Recent Activity
- ☑ Hash Lookup
- ☑ File Type Identification
- ☑ Extension Mismatch Detector
- ☑ Embedded File Extractor
- ☑ Exif Parser
- ☑ Keyword Search
- ☑ Email Parser
- ☑ Encryption Detection
- ☑ Interesting Files Identifier
- ☑ Correlation Engine
- ☑ PhotoRec Carver
- ☑ Virtual Machine Extractor
- ☑ Data Source Integrity

The selected module has no per-run settings.

Extracts recent user activity, such as Web browsing, recently us...

Figure 76: Configuring ingest modules.

Created “SSDImage_01.001” is selected and click on open, as shown in figure 75. In the next step, configure the ingest modules. These are nothing but different modules on which Autopsy is going to analyze. Modules can be enabled and disabled as per the examiner's concern.



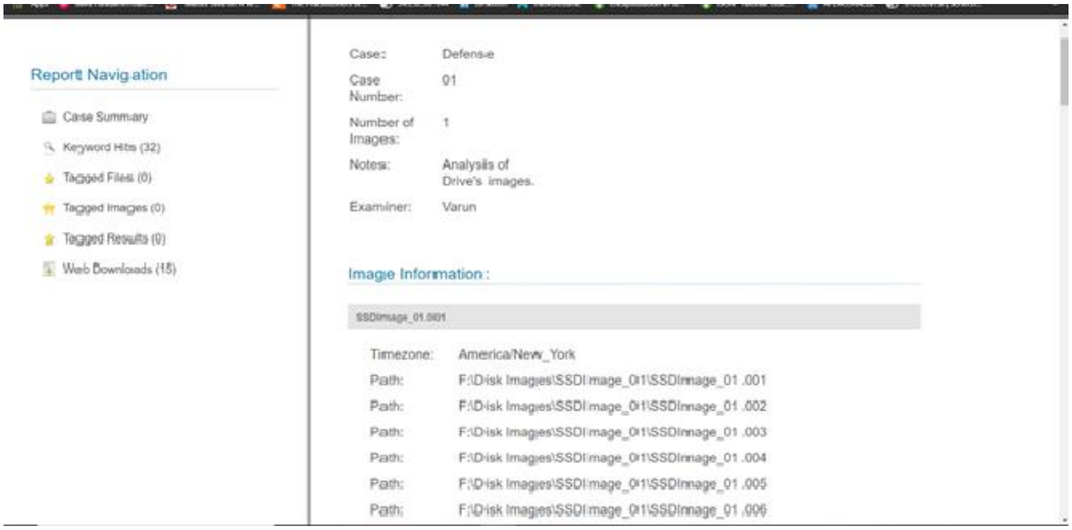
/img_SSDImage_01.001/Dummy Case Folder

16 Results

Name	S	C	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Know
[current folder]			2020-03-18 00:21:44 EDT	2020-03-18 00:21:45 EDT	2020-03-18 00:21:44 EDT	2020-03-18 00:21:44 EDT	56	Allocated	Allocated	unkno
[parent folder]			2020-03-18 00:21:53 EDT	2020-03-18 00:21:53 EDT	2020-03-18 00:21:53 EDT	2020-03-02 12:27:42 EST	56	Allocated	Allocated	unkno
Vctim's Face			2020-03-18 00:21:44 EDT	2020-03-18 00:21:44 EDT	2020-03-18 00:21:44 EDT	2020-03-18 00:21:44 EDT	520	Allocated	Allocated	unkno
Victim's car			2020-03-18 00:21:44 EDT	2020-03-18 00:21:44 EDT	2020-03-18 00:21:44 EDT	2020-03-18 00:21:44 EDT	608	Allocated	Allocated	unkno
Victim's House			2020-03-18 00:21:44 EDT	2020-03-18 00:21:44 EDT	2020-03-18 00:21:44 EDT	2020-03-18 00:21:44 EDT	280	Allocated	Allocated	unkno
Asia.jpg			2020-03-17 23:02:14 EDT	2020-03-17 23:54:30 EDT	2020-03-18 00:21:44 EDT	2020-03-18 00:21:44 EDT	10927	Allocated	Allocated	unkno
Asia.jpg:Zone.Identifier			2020-03-17 23:02:14 EDT	2020-03-17 23:54:30 EDT	2020-03-18 00:21:44 EDT	2020-03-18 00:21:44 EDT	50	Allocated	Allocated	unkno
DateofAction.pdf			2020-03-17 22:59:10 EDT	2020-03-17 23:22:05 EDT	2020-03-18 00:21:44 EDT	2020-03-18 00:21:44 EDT	26837	Allocated	Allocated	unkno
Dubai.jpg			2020-03-17 23:23:21 EDT	2020-03-17 23:54:30 EDT	2020-03-18 00:21:44 EDT	2020-03-18 00:21:44 EDT	9948	Allocated	Allocated	unkno
Dubai.jpg:Zone.Identifier			2020-03-17 23:23:21 EDT	2020-03-17 23:54:30 EDT	2020-03-18 00:21:44 EDT	2020-03-18 00:21:44 EDT	50	Allocated	Allocated	unkno
Europe.jpg			2020-03-17 23:01:44 EDT	2020-03-17 23:54:30 EDT	2020-03-18 00:21:44 EDT	2020-03-18 00:21:44 EDT	186034	Allocated	Allocated	unkno
Europe.jpg:Zone.Identifier			2020-03-17 23:01:44 EDT	2020-03-17 23:54:30 EDT	2020-03-18 00:21:44 EDT	2020-03-18 00:21:44 EDT	50	Allocated	Allocated	unkno
Pinned Locations.jpg			2020-03-17 23:04:04 EDT	2020-03-17 23:21:33 EDT	2020-03-18 00:21:44 EDT	2020-03-18 00:21:44 EDT	13515	Allocated	Allocated	unkno
Pinned Locations.jpg:Zone.Identifier			2020-03-17 23:04:04 EDT	2020-03-17 23:21:33 EDT	2020-03-18 00:21:44 EDT	2020-03-18 00:21:44 EDT	50	Allocated	Allocated	unkno
Travel Info.xlsx			2020-03-17 22:53:47 EDT	2020-03-17 22:53:47 EDT	2020-03-18 00:21:44 EDT	2020-03-18 00:21:44 EDT	9802	Allocated	Allocated	unkno
Victim's Identifications.docx			2020-03-17 22:32:09 EDT	2020-03-17 23:55:20 EDT	2020-03-18 00:21:44 EDT	2020-03-18 00:21:44 EDT	12407	Allocated	Allocated	unkno

Analyzing files from SSDImage_01.001 51%

Figure 77: Analyzing SSD image 1.



Case: Defense

Case Number: 01

Number of Images: 1

Notes: Analysis of Drive's images.

Examiner: Varun

Image Information:

SSDImage_01.001

Timezone: America/New_York

Path: F:\Disk Images\SSDImage_01\SSDImage_01.001

Path: F:\Disk Images\SSDImage_01\SSDImage_01.002

Path: F:\Disk Images\SSDImage_01\SSDImage_01.003

Path: F:\Disk Images\SSDImage_01\SSDImage_01.004

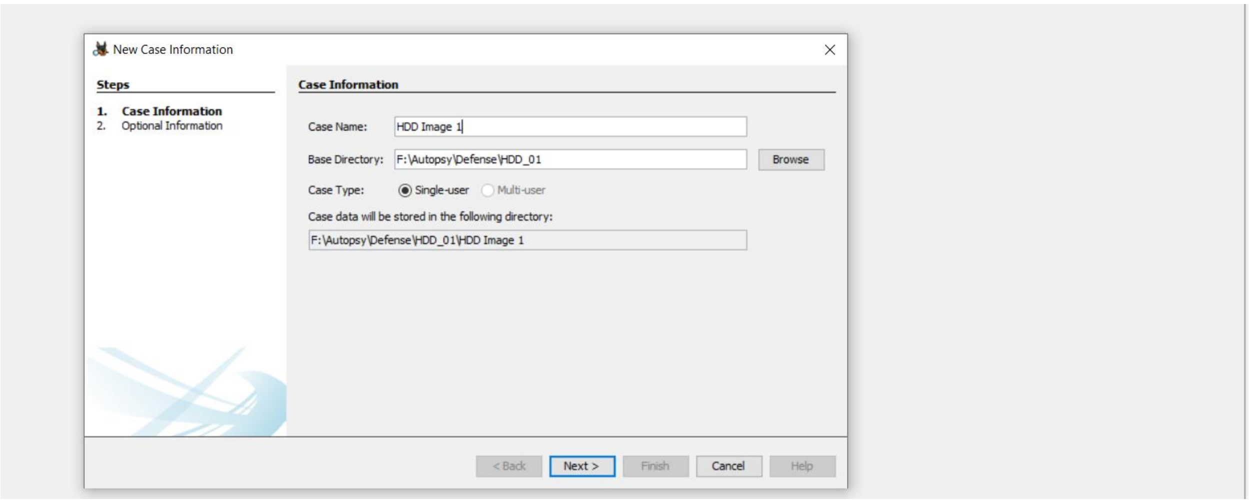
Path: F:\Disk Images\SSDImage_01\SSDImage_01.005

Path: F:\Disk Images\SSDImage_01\SSDImage_01.006

Figure 78: Final report generated by Autopsy for SSD image 1.

Usually, the time taken by Autopsy to analyze an image completely depends on the image size. For this 120 GB image, it took nearly 4 hours. The bottom right of image 77 shows the progress of image analysis, and a final report will be generated, as shown in figure 78.

Similar to what has been done above, the HDD image created before deleting any files is analyzed using Autopsy. Select the type of data source to add, i.e., the image file of respective HDD drive before deleting any files. A new case database and text index will be created.



Steps

1. Case Information
2. Optional Information

Case Information

Case Name: HDD Image 1

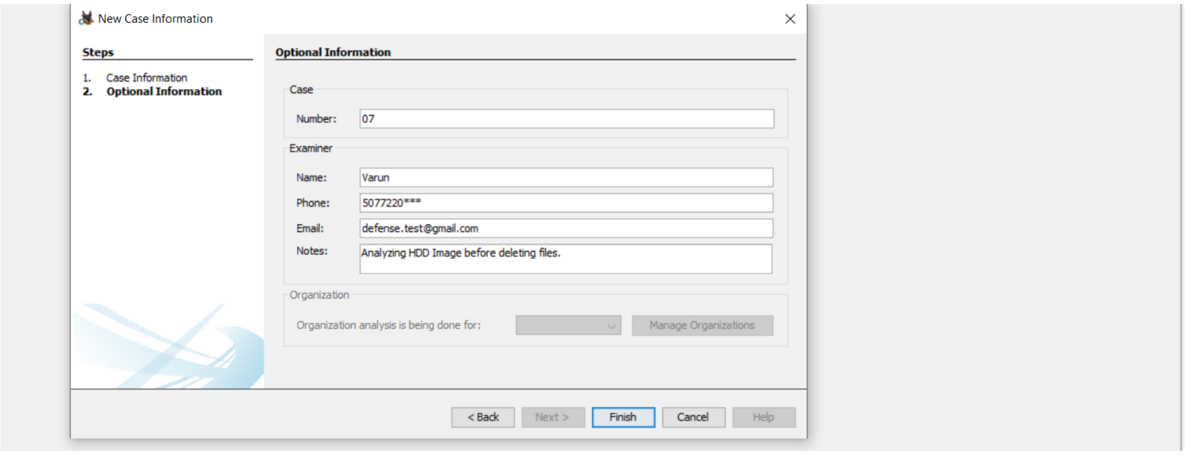
Base Directory: F:\Autopsy\Defense\HDD_01

Case Type: ● Single-user ○ Multi-user

Case data will be stored in the following directory:

F:\Autopsy\Defense\HDD_01\HDD Image 1

Figure 79: Enter case information for HDD image 1.



Steps

1. Case Information
2. Optional Information

Optional Information

Case

Number: 07

Examiner

Name: Varun

Phone: 5077220***

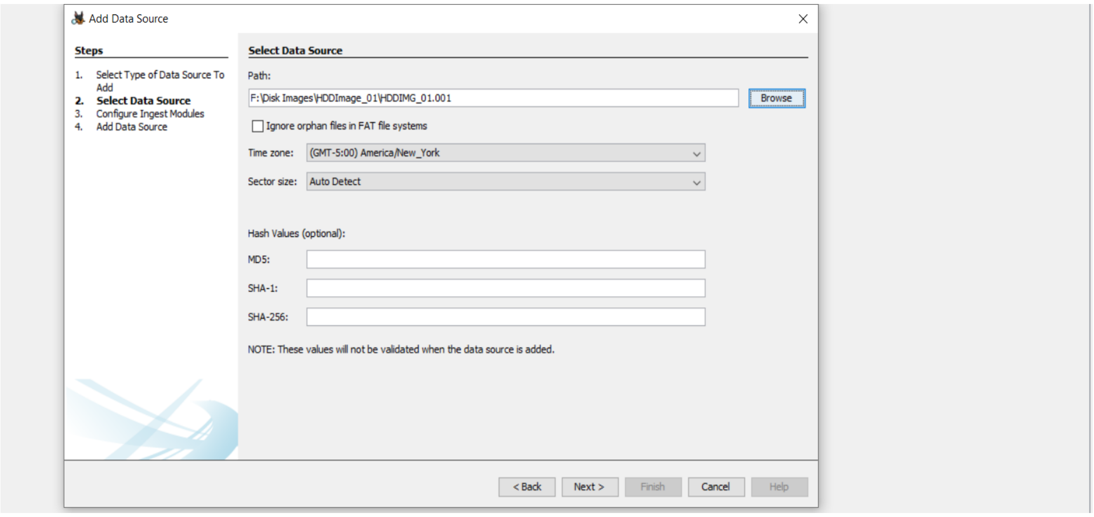
Email: defense.test@gmail.com

Notes: Analyzing HDD Image before deleting files.

Organization

Organization analysis is being done for:

Figure 80: Enter optional case information.



Add Data Source

Steps

1. Select Type of Data Source To Add
2. **Select Data Source**
3. Configure Ingest Modules
4. Add Data Source

Select Data Source

Path: F:\Disk Images\HDDImage_01\HDDIMG_01.001

□ Ignore orphan files in FAT file systems

Time zone: (GMT-5:00) America/New_York

Sector size: Auto Detect

Hash Values (optional):

MD5:

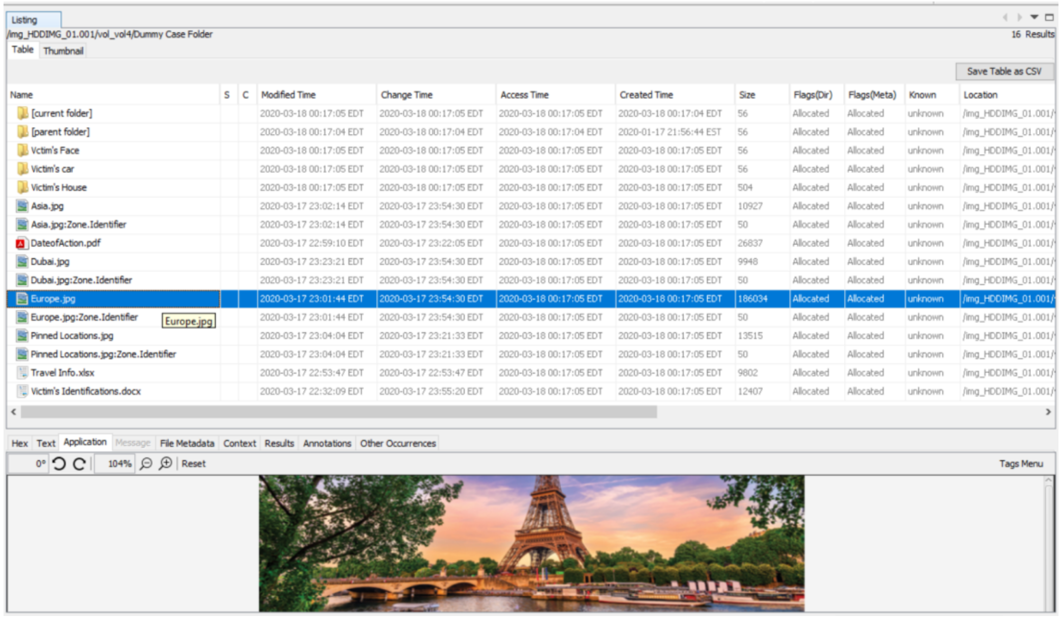
SHA-1:

SHA-256:

NOTE: These values will not be validated when the data source is added.

Figure 81: Select the Data source image path.

It is optional to enter the hash values. Click next to set the ingestion modules. The selected modules will be analyzed and displayed in the report. Selecting only specific and required modules can save time taking for Autopsy to completely analyze an image. For SSD, it takes 2 - 4 hours and for HDD 4 - 6 hours. Figure 82 shows case image after complete analysis.

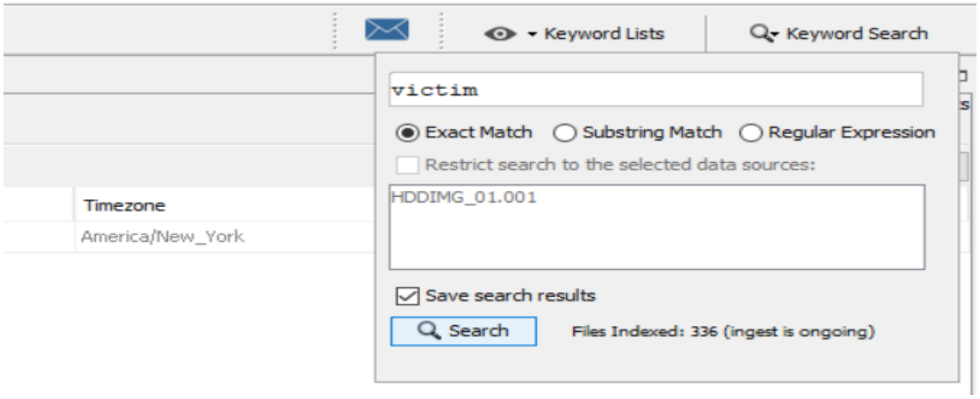


/img_HDDIMG_01.001/vol_vol4/Dummy Case Folder

16 Results

Name	S	C	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known	Location
[current folder]			2020-03-18 00:17:05 EDT	2020-03-18 00:17:05 EDT	2020-03-18 00:17:05 EDT	2020-03-18 00:17:04 EDT	56	Allocated	Allocated	unknown	/img_HDDIMG_01.001/
[parent folder]			2020-03-18 00:17:04 EDT	2020-03-18 00:17:04 EDT	2020-03-18 00:17:04 EDT	2020-01-17 21:56:44 EST	56	Allocated	Allocated	unknown	/img_HDDIMG_01.001/
Vctim's Face			2020-03-18 00:17:05 EDT	2020-03-18 00:17:05 EDT	2020-03-18 00:17:05 EDT	2020-03-18 00:17:05 EDT	56	Allocated	Allocated	unknown	/img_HDDIMG_01.001/
Victim's car			2020-03-18 00:17:05 EDT	2020-03-18 00:17:05 EDT	2020-03-18 00:17:05 EDT	2020-03-18 00:17:05 EDT	56	Allocated	Allocated	unknown	/img_HDDIMG_01.001/
Victim's House			2020-03-18 00:17:05 EDT	2020-03-18 00:17:05 EDT	2020-03-18 00:17:05 EDT	2020-03-18 00:17:05 EDT	504	Allocated	Allocated	unknown	/img_HDDIMG_01.001/
Asia.jpg			2020-03-17 23:02:14 EDT	2020-03-17 23:54:30 EDT	2020-03-18 00:17:05 EDT	2020-03-18 00:17:05 EDT	10927	Allocated	Allocated	unknown	/img_HDDIMG_01.001/
Asia.jpg:Zone.Identifier			2020-03-17 23:02:14 EDT	2020-03-17 23:54:30 EDT	2020-03-18 00:17:05 EDT	2020-03-18 00:17:05 EDT	50	Allocated	Allocated	unknown	/img_HDDIMG_01.001/
DateofAction.pdf			2020-03-17 22:59:10 EDT	2020-03-17 23:22:05 EDT	2020-03-18 00:17:05 EDT	2020-03-18 00:17:05 EDT	26837	Allocated	Allocated	unknown	/img_HDDIMG_01.001/
Dubai.jpg			2020-03-17 23:23:21 EDT	2020-03-17 23:54:30 EDT	2020-03-18 00:17:05 EDT	2020-03-18 00:17:05 EDT	9948	Allocated	Allocated	unknown	/img_HDDIMG_01.001/
Dubai.jpg:Zone.Identifier			2020-03-17 23:23:21 EDT	2020-03-17 23:54:30 EDT	2020-03-18 00:17:05 EDT	2020-03-18 00:17:05 EDT	50	Allocated	Allocated	unknown	/img_HDDIMG_01.001/
Europe.jpg			2020-03-17 23:01:44 EDT	2020-03-17 23:54:30 EDT	2020-03-18 00:17:05 EDT	2020-03-18 00:17:05 EDT	186034	Allocated	Allocated	unknown	/img_HDDIMG_01.001/
Europe.jpg:Zone.Identifier			2020-03-17 23:01:44 EDT	2020-03-17 23:54:30 EDT	2020-03-18 00:17:05 EDT	2020-03-18 00:17:05 EDT	50	Allocated	Allocated	unknown	/img_HDDIMG_01.001/
Pinned Locations.jpg			2020-03-17 23:04:04 EDT	2020-03-17 23:21:33 EDT	2020-03-18 00:17:05 EDT	2020-03-18 00:17:05 EDT	13515	Allocated	Allocated	unknown	/img_HDDIMG_01.001/
Pinned Locations.jpg:Zone.Identifier			2020-03-17 23:04:04 EDT	2020-03-17 23:21:33 EDT	2020-03-18 00:17:05 EDT	2020-03-18 00:17:05 EDT	50	Allocated	Allocated	unknown	/img_HDDIMG_01.001/
Travel Info.xlsx			2020-03-17 22:53:47 EDT	2020-03-17 22:53:47 EDT	2020-03-18 00:17:05 EDT	2020-03-18 00:17:05 EDT	9802	Allocated	Allocated	unknown	/img_HDDIMG_01.001/
Victim's Identifications.docx			2020-03-17 22:32:09 EDT	2020-03-17 23:55:20 EDT	2020-03-18 00:17:05 EDT	2020-03-18 00:17:05 EDT	12407	Allocated	Allocated	unknown	/img_HDDIMG_01.001/

Figure 82: Case content viewed after analyzing.



Timezone
America/New_York

victim

● Exact Match ○ Substring Match ○ Regular Expression

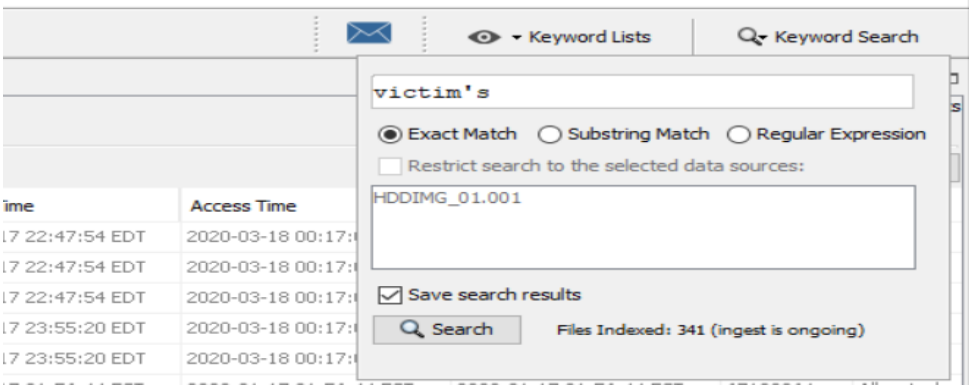
□ Restrict search to the selected data sources:

HDDIMG_01.001

☑ Save search results

Files Indexed: 336 (ingest is ongoing)

Figure 83: Keyword search for word victim.



victim's

● Exact Match ○ Substring Match ○ Regular Expression

□ Restrict search to the selected data sources:

HDDIMG_01.001

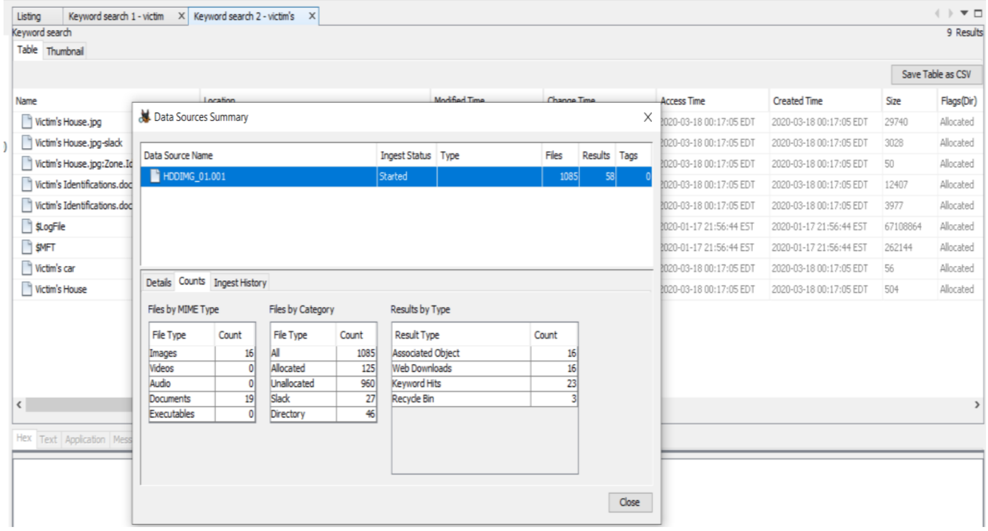
☑ Save search results

Search

Files Indexed: 341 (ingest is ongoing)

ime	Access Time
17 22:47:54 EDT	2020-03-18 00:17:
17 22:47:54 EDT	2020-03-18 00:17:
17 22:47:54 EDT	2020-03-18 00:17:
17 23:55:20 EDT	2020-03-18 00:17:
17 23:55:20 EDT	2020-03-18 00:17:

Figure 84: Keyword search for word “victim's”.



9 Results

Name	Access Time	Created Time	Size	Flags(Dir)
Victim's House.jpg	2020-03-18 00:17:05 EDT	2020-03-18 00:17:05 EDT	29740	Allocated
Victim's House.jpg-slack	2020-03-18 00:17:05 EDT	2020-03-18 00:17:05 EDT	3028	Allocated
Victim's House.jpg:Zone.Id	2020-03-18 00:17:05 EDT	2020-03-18 00:17:05 EDT	50	Allocated
Victim's Identifications.doc	2020-03-18 00:17:05 EDT	2020-03-18 00:17:05 EDT	12407	Allocated
Victim's Identifications.doc	2020-03-18 00:17:05 EDT	2020-03-18 00:17:05 EDT	3977	Allocated
$LogFile	2020-01-17 21:56:44 EST	2020-01-17 21:56:44 EST	67108864	Allocated
$MFT	2020-01-17 21:56:44 EST	2020-01-17 21:56:44 EST	262144	Allocated
Victim's car	2020-03-18 00:17:05 EDT	2020-03-18 00:17:05 EDT	56	Allocated
Victim's House	2020-03-18 00:17:05 EDT	2020-03-18 00:17:05 EDT	504	Allocated

Data Sources Summary

Data Source Name	Ingest Status	Type	Files	Results	Tags
HDDIMG_01.001	Started		1085	58	0

Files by MIME Type

File Type	Count
Images	16
Videos	0
Audio	0
Documents	19
Executables	0

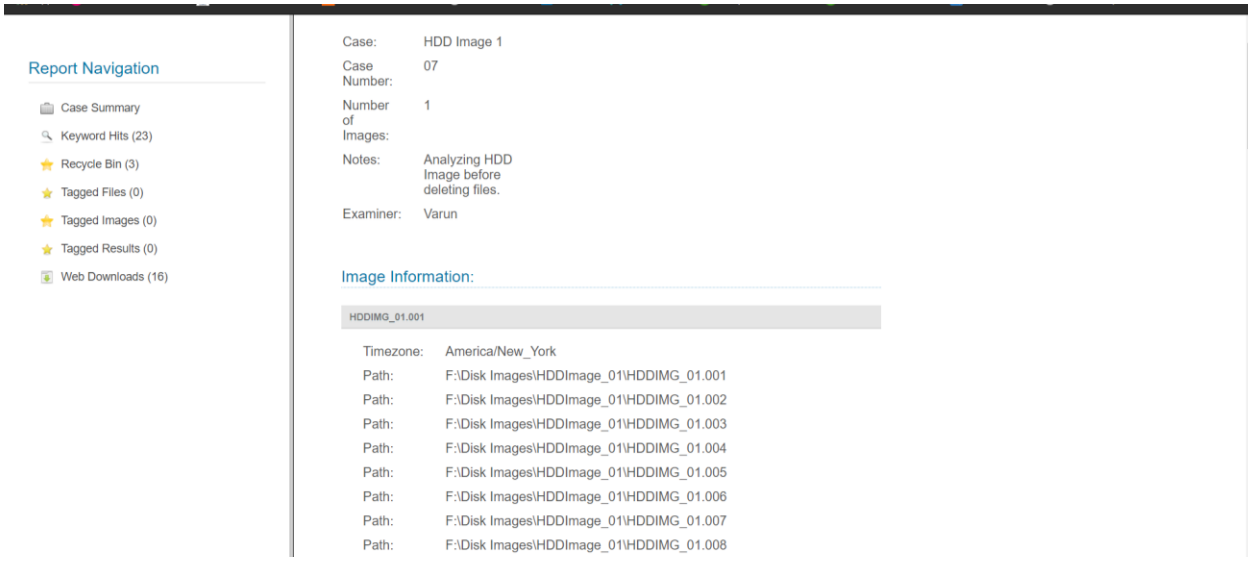
Files by Category

File Type	Count
All	1085
Allocated	125
Unallocated	960
Slack	27
Directory	46

Results by Type

Result Type	Count
Associated Object	16
Web Downloads	16
Keyword Hits	23
Recycle Bin	3

Figure 85: Data source summary for HDD image 1.



Case: HDD Image 1
Case Number: 07
Number of Images: 1
Notes: Analyzing HDD Image before deleting files.
Examiner: Varun

Image Information:

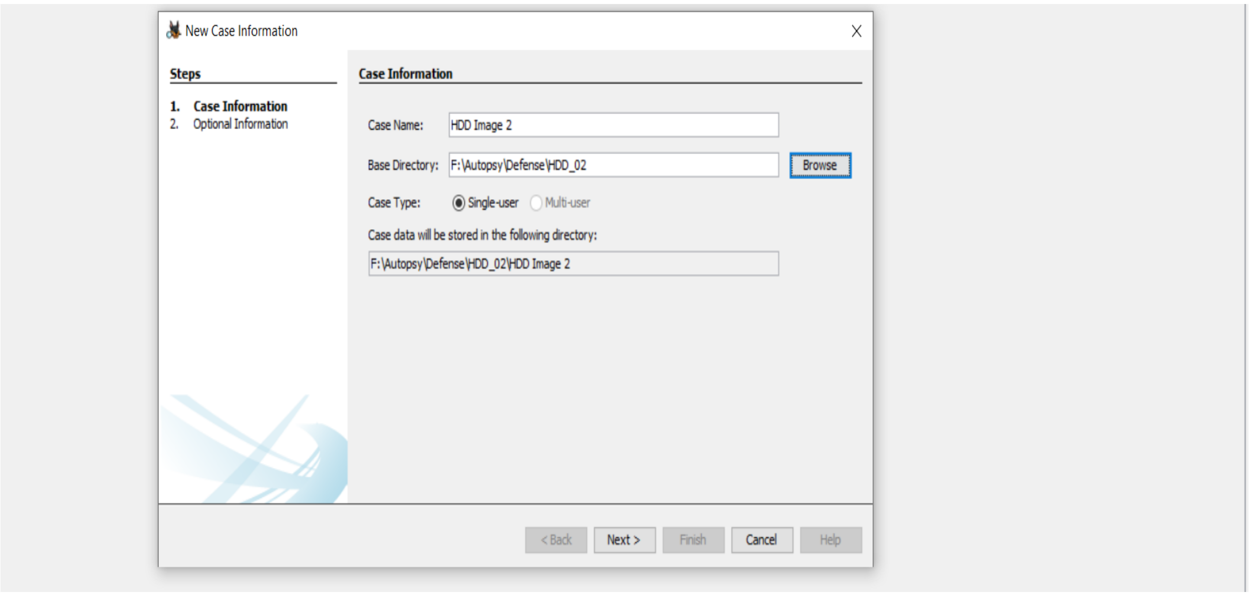
HDDIMG_01.001

Timezone:	America/New_York
Path:	F:\Disk Images\HDDImage_01\HDDIMG_01.001
Path:	F:\Disk Images\HDDImage_01\HDDIMG_01.002
Path:	F:\Disk Images\HDDImage_01\HDDIMG_01.003
Path:	F:\Disk Images\HDDImage_01\HDDIMG_01.004
Path:	F:\Disk Images\HDDImage_01\HDDIMG_01.005
Path:	F:\Disk Images\HDDImage_01\HDDIMG_01.006
Path:	F:\Disk Images\HDDImage_01\HDDIMG_01.007
Path:	F:\Disk Images\HDDImage_01\HDDIMG_01.008

Figure 86: Final report generated for HDD image 1.

In figure 82, after the image has been analyzed completely, “Europe.jpg” is double-clicked to view the picture. The bottom of the tool displays the picture. The next step is searching for keywords. In this study, two keywords “victim” and “victim’s” is searched; this is shown in figures 83, 84. After the files related to the keywords have been listed, a data source summary is generated. This is shown in figure 85. From this figure the keyword count is 23 and the web downloaded content is 16. This is all what is present in the dummy case folder. Figure 86 shows a final web report generated by Autopsy for HDD image 1. By this stage both the drives SSD’s and HDD’s image 1 has been analyzed using Autopsy forensic tool.

Now the same tool is used for analyzing the images created from HDD and SSD after deleting evidence files. This image 2 of respective drives will be loaded, analyzed and reports are generated. These reports provide the total number of files in the drives, deleted files, searched keywords hits etc. This data will be noted for further sections, where all the results will be tabulated and discussed in detail. Starting with HDD image 2 analysis, steps undertaken are shown below.



Steps

1. **Case Information**
2. Optional Information

Case Information

Case Name: HDD Image 2

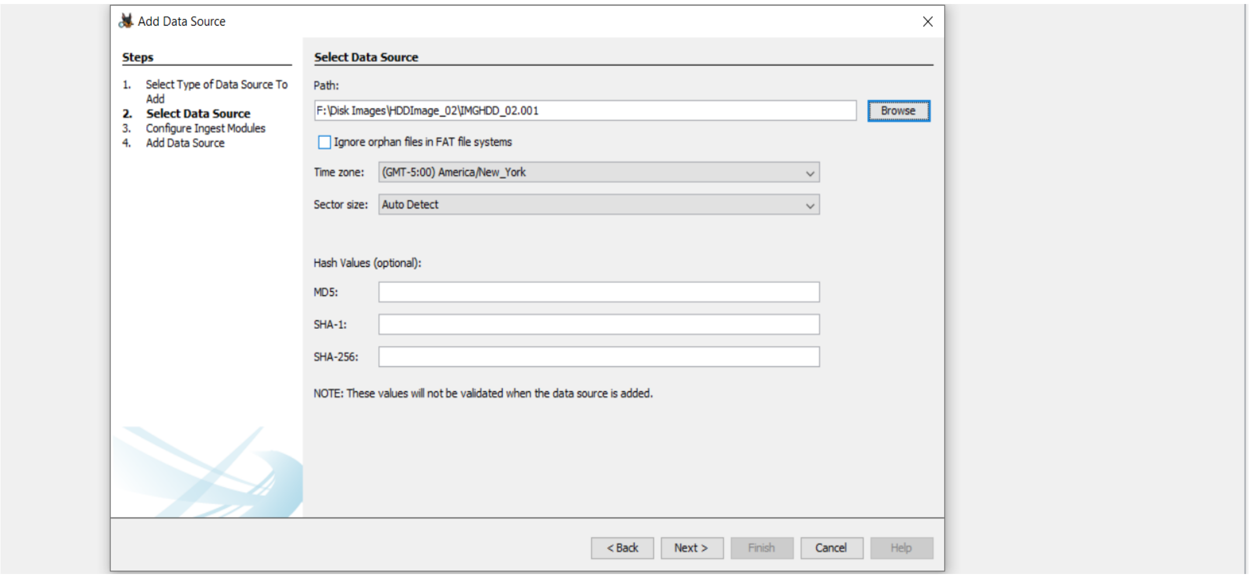
Base Directory: F:\Autopsy\Defense\HDD_02

Case Type: ● Single-user ○ Multi-user

Case data will be stored in the following directory:

F:\Autopsy\Defense\HDD_02\HDD Image 2

Figure 87: Adding HDD image 2 information.



Steps

1. Select Type of Data Source To Add
2. **Select Data Source**
3. Configure Ingest Modules
4. Add Data Source

Select Data Source

Path:

F:\Disk Images\HDDImage_02\IMGHDD_02.001

□ Ignore orphan files in FAT file systems

Time zone: (GMT-5:00) America/New_York

Sector size: Auto Detect

Hash Values (optional):

MD5:

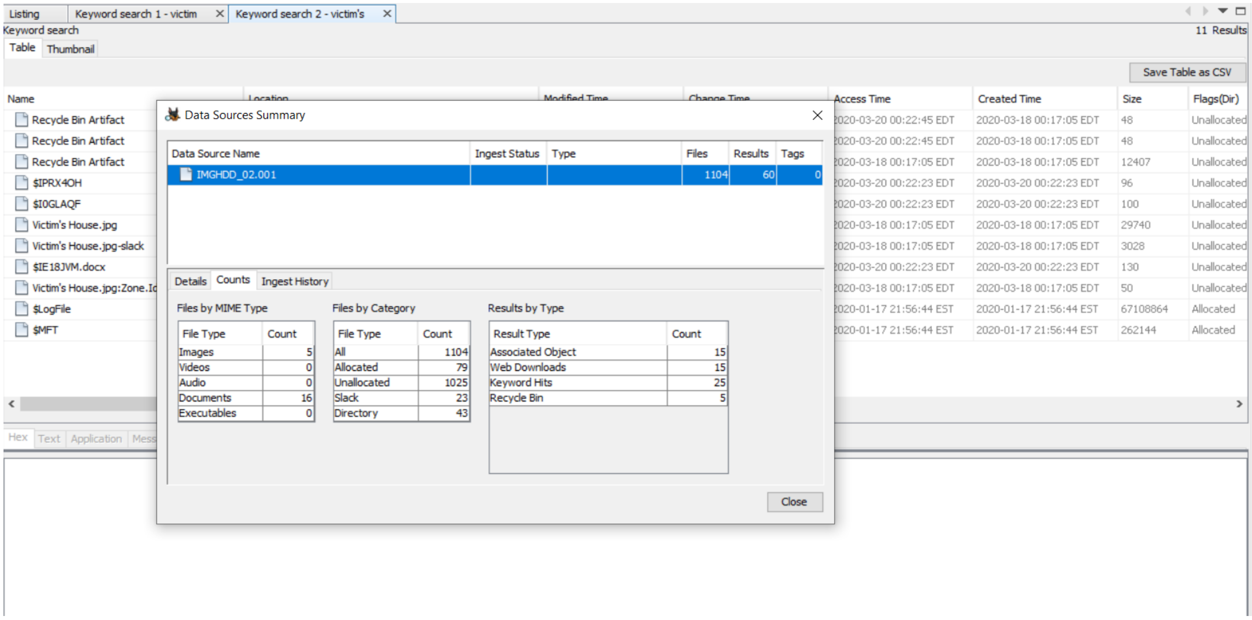
SHA-1:

SHA-256:

NOTE: These values will not be validated when the data source is added.

Figure 88: Selecting source data as HDD image 2.

HDD Image 2 is selected as a source data that will be analyzed, and this is shown in figures 87 and 88. After the analysis is completed, the examiner looks for keywords search. After the keywords are searched, and hits are generated, a data source summary is generated, as shown in figure 89.



Name	Access Time	Created Time	Size	Flags(Dir)
Recycle Bin Artifact	2020-03-20 00:22:45 EDT	2020-03-18 00:17:05 EDT	48	Unallocated
Recycle Bin Artifact	2020-03-20 00:22:45 EDT	2020-03-18 00:17:05 EDT	48	Unallocated
Recycle Bin Artifact	2020-03-18 00:17:05 EDT	2020-03-18 00:17:05 EDT	12407	Unallocated
$IPRX4OH	2020-03-20 00:22:23 EDT	2020-03-20 00:22:23 EDT	96	Unallocated
$I0GLAQF	2020-03-20 00:22:23 EDT	2020-03-20 00:22:23 EDT	100	Unallocated
Victim's House.jpg	2020-03-18 00:17:05 EDT	2020-03-18 00:17:05 EDT	29740	Unallocated
Victim's House.jpg-slack	2020-03-18 00:17:05 EDT	2020-03-18 00:17:05 EDT	3028	Unallocated
$IE18JVM.docx	2020-03-20 00:22:23 EDT	2020-03-20 00:22:23 EDT	130	Unallocated
Victim's House.jpg:Zone.Id	2020-03-18 00:17:05 EDT	2020-03-18 00:17:05 EDT	50	Unallocated
$LogFile	2020-01-17 21:56:44 EST	2020-01-17 21:56:44 EST	67108864	Allocated
$MFT	2020-01-17 21:56:44 EST	2020-01-17 21:56:44 EST	262144	Allocated

Data Sources Summary

Data Source Name	Ingest Status	Type	Files	Results	Tags
IMGHDD_02.001			1104	60	0

Files by MIME Type

File Type	Count
Images	5
Videos	0
Audio	0
Documents	16
Executables	0

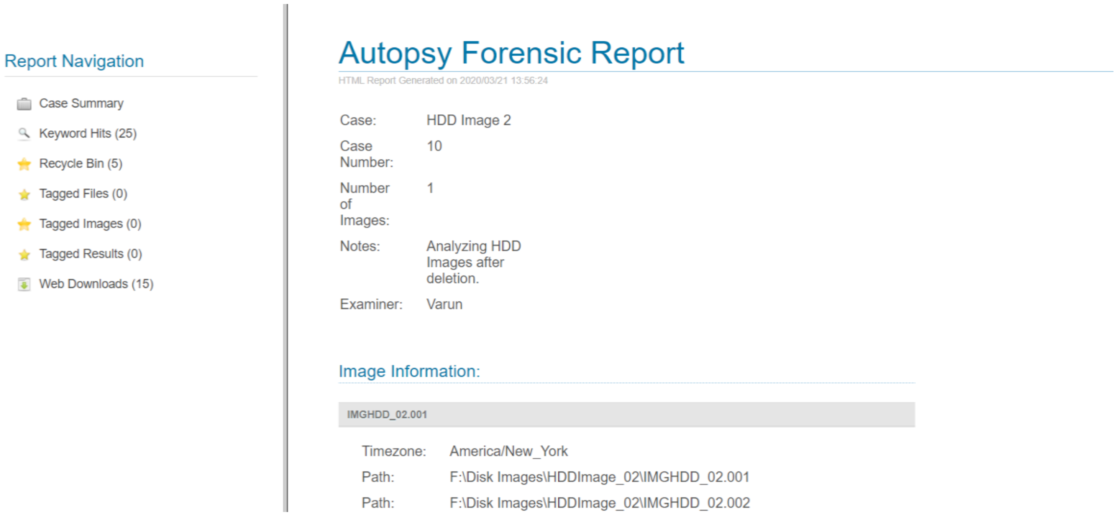
Files by Category

File Type	Count
All	1104
Allocated	79
Unallocated	1025
Slack	23
Directory	43

Results by Type

Result Type	Count
Associated Object	15
Web Downloads	15
Keyword Hits	25
Recycle Bin	5

Figure 89: Data source summary.



Autopsy Forensic Report

HTML Report Generated on 2020/03/21 13:56:24

Case:	HDD Image 2
Case Number:	10
Number of Images:	1
Notes:	Analyzing HDD Images after deletion.
Examiner:	Varun

Image Information:

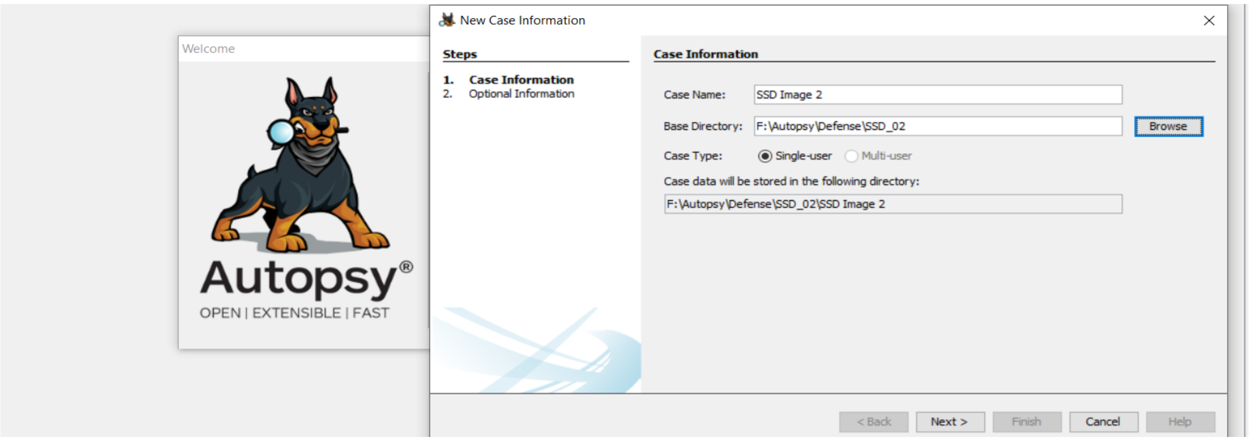
IMGHDD_02.001

Timezone:	America/New_York
Path:	F:\Disk Images\HDDImage_02\IMGHDD_02.001
Path:	F:\Disk Images\HDDImage_02\IMGHDD_02.002

Figure 90: Final report generated for HDD image 2.

The final report generated after all the steps are followed is shown in figure 90. Similarly, an analysis of SSD image 2 is done in the next few steps.

The last image analyzed using Autopsy is SSD image 2. The analysis of this image plays a major role in this study. The results obtained will be analyzed, observed, and discussed in the next chapter. The process of analysis is shown in the figures below. Provide the case information and examiner details as the first steps in this process.



New Case Information

Steps

1. **Case Information**
2. Optional Information

Case Information

Case Name: SSD Image 2

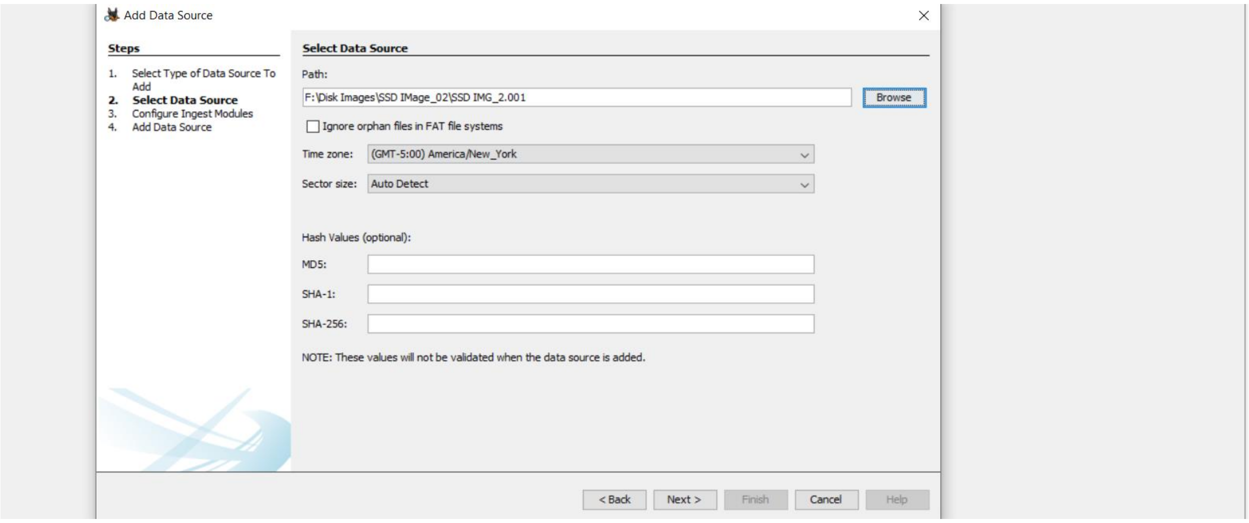
Base Directory: F:\Autopsy\Defense\SSD_02

Case Type: ● Single-user ○ Multi-user

Case data will be stored in the following directory:

F:\Autopsy\Defense\SSD_02\SSD Image 2

Figure 91: Adding new case information for SSD image 2.



Add Data Source

Steps

1. Select Type of Data Source To Add
2. **Select Data Source**
3. Configure Ingest Modules
4. Add Data Source

Select Data Source

Path:

F:\Disk Images\SSD IMage_02\SSD IMG_2.001

□ Ignore orphan files in FAT file systems

Time zone: (GMT-5:00) America/New_York

Sector size: Auto Detect

Hash Values (optional):

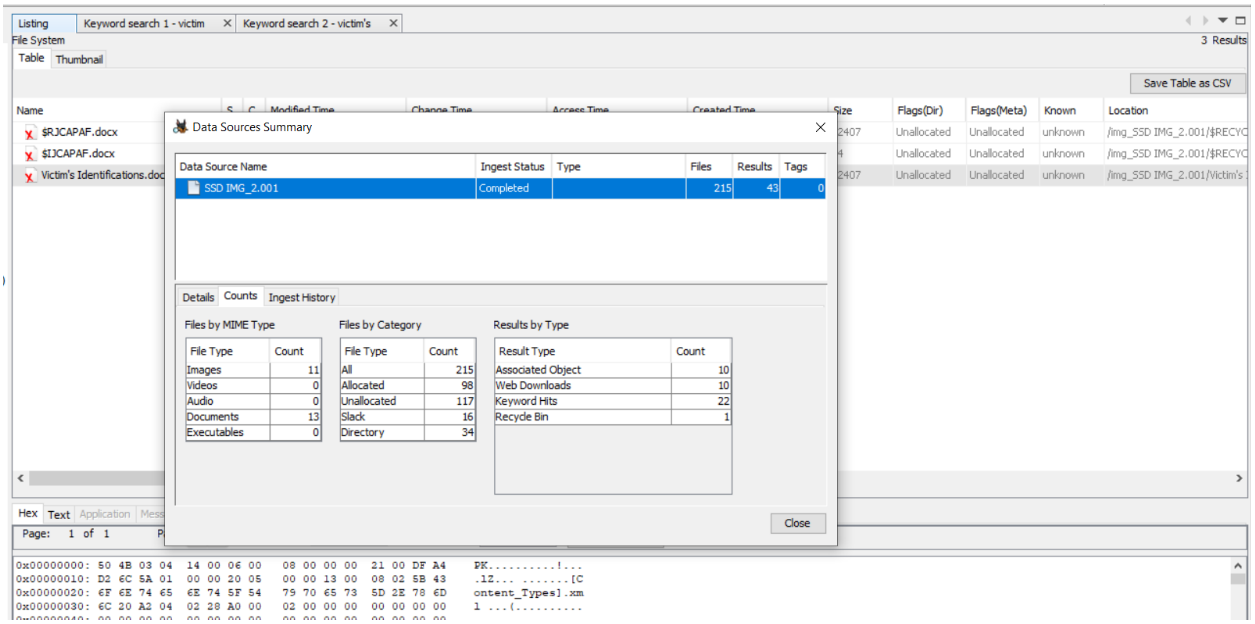
MD5:

SHA-1:

SHA-256:

NOTE: These values will not be validated when the data source is added.

Figure 92: Selecting data source SSD image 2.



Name	S	C	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known	Location
$RJCAPAF.docx							2407	Unallocated	Unallocated	unknown	/img_SSD IMG_2.001/$RECYC
$IJCAPAF.docx							4	Unallocated	Unallocated	unknown	/img_SSD IMG_2.001/$RECYC
Victim's Identifications.doc							2407	Unallocated	Unallocated	unknown	/img_SSD IMG_2.001/Victim's

Data Sources Summary

Data Source Name	Ingest Status	Type	Files	Results	Tags
SSD IMG_2.001	Completed		215	43	0

Files by MIME Type

File Type	Count
Images	11
Videos	0
Audio	0
Documents	13
Executables	0

Files by Category

File Type	Count
All	215
Allocated	98
Unallocated	117
Slack	16
Directory	34

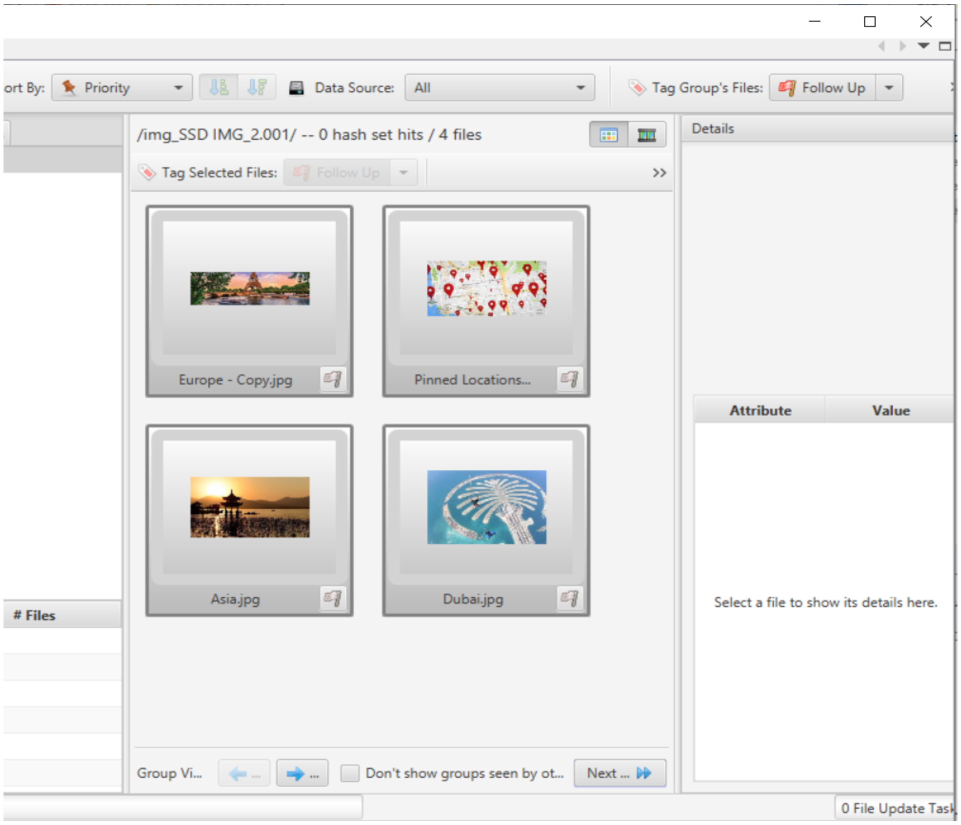
Results by Type

Result Type	Count
Associated Object	10
Web Downloads	10
Keyword Hits	22
Recycle Bin	1

Page: 1 of 1

```
0x00000000: 50 4B 03 04  14 00 06 00   08 00 00 00  21 00 DF A4    PK..........!...
0x00000010: D2 6C 5A 01  00 00 20 05   00 00 13 00  08 02 5B 43    .lZ... .......[C
0x00000020: 6F 6E 74 65  6E 74 5F 54   79 70 65 73  5D 2E 78 6D    ontent_Types].xm
0x00000030: 6C 20 A2 04  02 28 A0 00   02 00 00 00  00 00 00 00    l ...(..........
```

Figure 93: Data source summary.

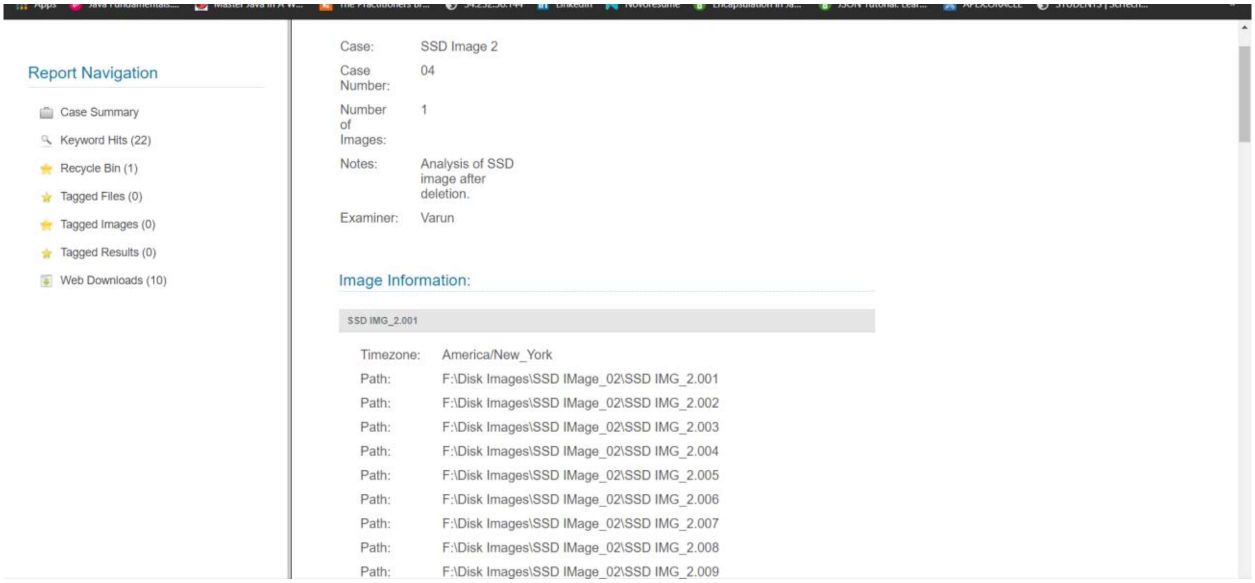


/img_SSD IMG_2.001/ -- 0 hash set hits / 4 files

Select a file to show its details here.

Figure 94: Files extracted from SSD image 2.

After the SSD image 2 analysis is completed, and keywords are searched, a data source summary report is viewed, as shown in figure 93. Apart from the evidence files deleted, the other files in the case folder were extracted and viewed in image 94. Investigator was not able to retrieve all the deleted files that were extracted from SSD image 2. The results are observed and discussed in the next chapter. Below figure 95, is a web report generated from Autopsy, with keyword hits being displayed.



Case: SSD Image 2
Case Number: 04
Number of Images: 1
Notes: Analysis of SSD image after deletion.
Examiner: Varun

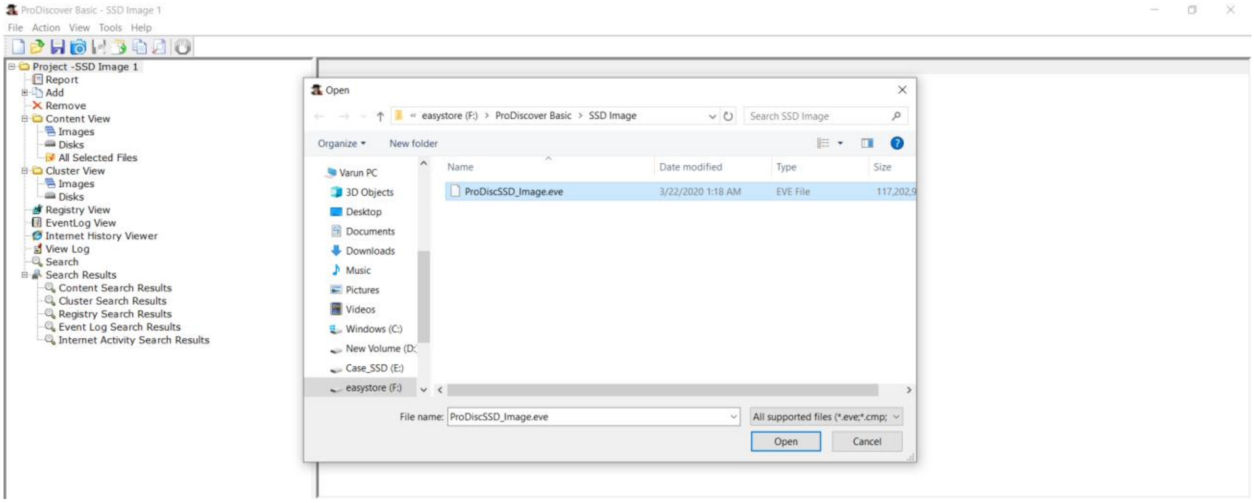
Image Information:

SSD IMG_2.001

Timezone: America/New_York
Path: F:\Disk Images\SSD IMage_02\SSD IMG_2.001
Path: F:\Disk Images\SSD IMage_02\SSD IMG_2.002
Path: F:\Disk Images\SSD IMage_02\SSD IMG_2.003
Path: F:\Disk Images\SSD IMage_02\SSD IMG_2.004
Path: F:\Disk Images\SSD IMage_02\SSD IMG_2.005
Path: F:\Disk Images\SSD IMage_02\SSD IMG_2.006
Path: F:\Disk Images\SSD IMage_02\SSD IMG_2.007
Path: F:\Disk Images\SSD IMage_02\SSD IMG_2.008
Path: F:\Disk Images\SSD IMage_02\SSD IMG_2.009

Figure 95: Final image generated for SSD Image 2 from Autopsy.

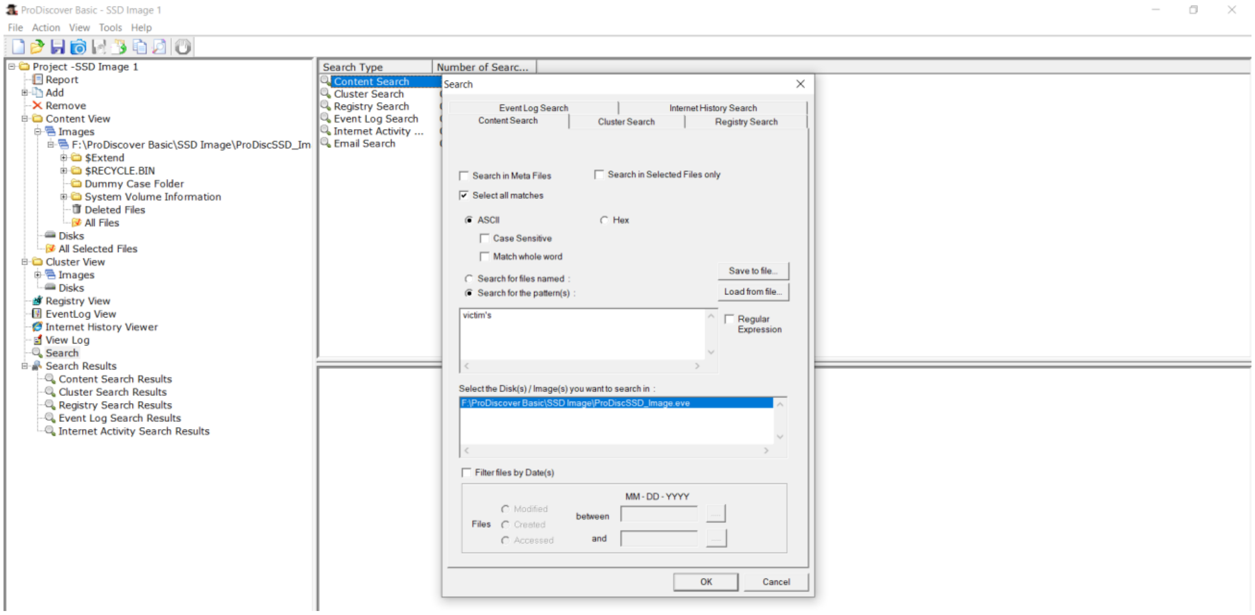
By this stage, all the HDD and SSD images created using FTK imager before deleting evidence files are shown in figures 41 and 47. Images created after deleting evidence files from SSD and HDD are shown in figures 55 and 65. After analyzing all the four images in Autopsy, the analysis steps are explained, and the results obtained will be discussed in the next chapter. Besides using FTK Imager for creating image and Autopsy for analyzing these images, the other forensic tool used in this experiment is ProDiscover Basic. Many research study's experimented and proved that data deleted on HDD can be retrieved using ProDiscover Basic. Thus, this study concentrates more on SSD and its behavior when exposed to ProDiscover Basic; steps performed to create an image are explained in the previous section. Figure 70 shows the ".eve" image file created from this tool. This image will be added to the tool, as shown in figure 96, and the analysis will be shown in the figures below.



Name	Date modified	Type	Size
ProDiscSSD_Image.eve	3/22/2020 1:18 AM	EVE File	117,202,9

File name: ProDiscSSD_Image.eve
All supported files (*.eve;*.cmp;

Figure 96: Adding SSD image to ProDiscover Basic.



□ Search in Meta Files
□ Search in Selected Files only
☑ Select all matches
● ASCII ○ Hex
□ Case Sensitive
□ Match whole word
○ Search for files named :
● Search for the pattern(s) :
victim's
□ Regular Expression
Select the Disk(s) / Image(s) you want to search in :
F:\ProDiscover Basic\SSD Image\ProDiscSSD_Image.eve
□ Filter files by Date(s)
MM - DD - YYYY
Files ○ Modified ○ Created ○ Accessed between and

Figure 97: Searching for keywords in ProDiscover Basic.

After the image is analyzed, the investigator performs keywords search, and no words are matched. This is shown in figure 98.

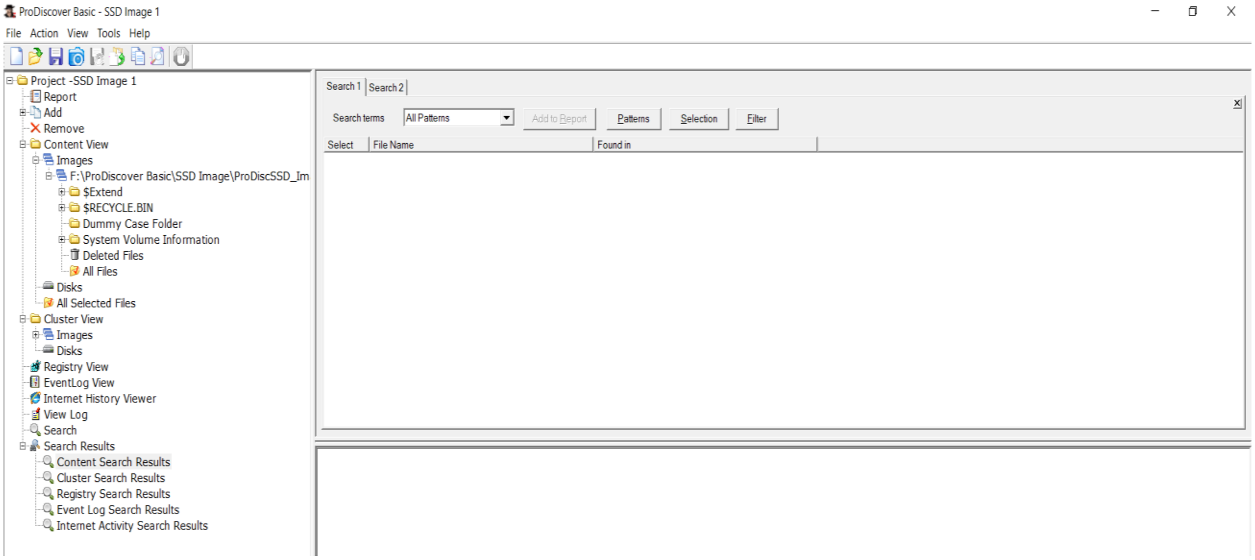


Figure 98: No keywords matched in the SSD image.

Summary

This chapter discussed more about how data is presented and analyzed in this experiment. At first, a dummy case folder is created, and this folder is copied to empty HDD and SSD. Later these drives images are extracted using the FTK Imager tool. The other set of images are extracted from drives using the same tool, after deleting some evidence files from both drives. These images are analyzed using Autopsy forensic tool, results obtained are observed and noted to discuss in the next chapter. Another image of SSD is created using ProDiscover basic tool, and the same tool is used to analyze the image to understand the behavior of the drive. Files deleted from HDD can be retrieved, and from SSD, most of the deleted files were lost, wiped out. The next chapter discusses more about what has been observed from the results obtained.

Chapter V: Results, Conclusion, and Recommendations.

Introduction

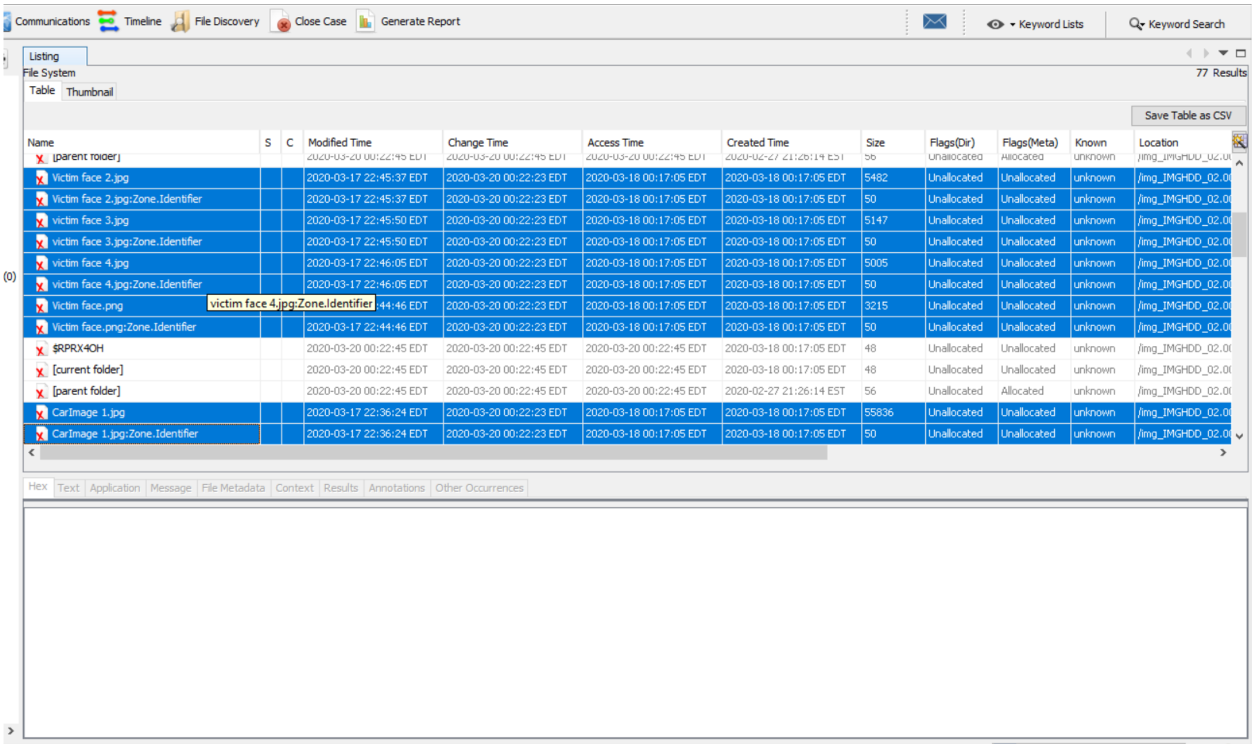
A forensic investigator gathers all the evidence related to the case and performs some forensic operations to extract the respective drive image. This image is then added to different forensic tools for further analysis, and different result sets will be analyzed. Similarly, as the last step of this study, this chapter discusses the results obtained from HDD and SSD in phases 1, 2. A conclusion to this study will be provided after the results are explained, and any further future study related to this study will be discussed at the end of this chapter.

Results

The results obtained by analyzing all the images used in this study will be discussed here. From chapter IV, it was clear that Autopsy and ProDiscover Basic tools were used for analyzing the images created. The data presentation of this study was presented in two phases. In the first phase, a case folder is created and copied to HDD, SSD. After copying, an image each of both drives is created using FTK Imager. This is shown in figure 41 for SSD and figure 47 for HDD. In the second phase, few evidence files from both drives are deleted, as shown in figures 49 and 57. The image created using the ProDiscover Basic tool is shown in figure 70.

The results obtained using Autopsy for each image will be explained below. Before deleting evidence files, after the analysis is completed, the keywords “victim” and “victim’s” are searched to see if files with those names will be displayed or not? The answer is “YES,” the files were displayed because all the files in the case folder can be viewed, and keyword hits count is noted from the generated web report, as shown in figures 78 and 86. All the keyword search hits will be compared and tabulated in table 5.

Analyzing images created after deleting evidence files from drives showed a difference. After analyzing the HDD image 2, all the deleted files were extracted and can be viewed as shown in figure 99. The keyword hits shown after searching for the keywords “victim” and “victim’s” are noted and will be compared in table 5 below.



Name	S	C	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known	Location
[parent folder]			2020-03-20 00:22:45 EDT	2020-03-20 00:22:45 EDT	2020-03-20 00:22:45 EDT	2020-02-27 21:26:14 EST	56	Unallocated	Allocated	unknown	/img_IMGHDD_02.0
Victim face 2.jpg			2020-03-17 22:45:37 EDT	2020-03-20 00:22:23 EDT	2020-03-18 00:17:05 EDT	2020-03-18 00:17:05 EDT	5482	Unallocated	Unallocated	unknown	/img_IMGHDD_02.0
Victim face 2.jpg:Zone.Identifier			2020-03-17 22:45:37 EDT	2020-03-20 00:22:23 EDT	2020-03-18 00:17:05 EDT	2020-03-18 00:17:05 EDT	50	Unallocated	Unallocated	unknown	/img_IMGHDD_02.0
victim face 3.jpg			2020-03-17 22:45:50 EDT	2020-03-20 00:22:23 EDT	2020-03-18 00:17:05 EDT	2020-03-18 00:17:05 EDT	5147	Unallocated	Unallocated	unknown	/img_IMGHDD_02.0
victim face 3.jpg:Zone.Identifier			2020-03-17 22:45:50 EDT	2020-03-20 00:22:23 EDT	2020-03-18 00:17:05 EDT	2020-03-18 00:17:05 EDT	50	Unallocated	Unallocated	unknown	/img_IMGHDD_02.0
victim face 4.jpg			2020-03-17 22:46:05 EDT	2020-03-20 00:22:23 EDT	2020-03-18 00:17:05 EDT	2020-03-18 00:17:05 EDT	5005	Unallocated	Unallocated	unknown	/img_IMGHDD_02.0
victim face 4.jpg:Zone.Identifier			2020-03-17 22:46:05 EDT	2020-03-20 00:22:23 EDT	2020-03-18 00:17:05 EDT	2020-03-18 00:17:05 EDT	50	Unallocated	Unallocated	unknown	/img_IMGHDD_02.0
Victim face.png			:44:46 EDT	2020-03-20 00:22:23 EDT	2020-03-18 00:17:05 EDT	2020-03-18 00:17:05 EDT	3215	Unallocated	Unallocated	unknown	/img_IMGHDD_02.0
Victim face.png:Zone.Identifier			2020-03-17 22:44:46 EDT	2020-03-20 00:22:23 EDT	2020-03-18 00:17:05 EDT	2020-03-18 00:17:05 EDT	50	Unallocated	Unallocated	unknown	/img_IMGHDD_02.0
$RPRX4OH			2020-03-20 00:22:45 EDT	2020-03-20 00:22:45 EDT	2020-03-20 00:22:45 EDT	2020-03-18 00:17:05 EDT	48	Unallocated	Unallocated	unknown	/img_IMGHDD_02.0
[current folder]			2020-03-20 00:22:45 EDT	2020-03-20 00:22:45 EDT	2020-03-20 00:22:45 EDT	2020-03-18 00:17:05 EDT	48	Unallocated	Unallocated	unknown	/img_IMGHDD_02.0
[parent folder]			2020-03-20 00:22:45 EDT	2020-03-20 00:22:45 EDT	2020-03-20 00:22:45 EDT	2020-02-27 21:26:14 EST	56	Unallocated	Allocated	unknown	/img_IMGHDD_02.0
CarImage 1.jpg			2020-03-17 22:36:24 EDT	2020-03-20 00:22:23 EDT	2020-03-18 00:17:05 EDT	2020-03-18 00:17:05 EDT	55836	Unallocated	Unallocated	unknown	/img_IMGHDD_02.0
CarImage 1.jpg:Zone.Identifier			2020-03-17 22:36:24 EDT	2020-03-20 00:22:23 EDT	2020-03-18 00:17:05 EDT	2020-03-18 00:17:05 EDT	50	Unallocated	Unallocated	unknown	/img_IMGHDD_02.0

Figure 99: Deleted files extracted from HDD image 2.

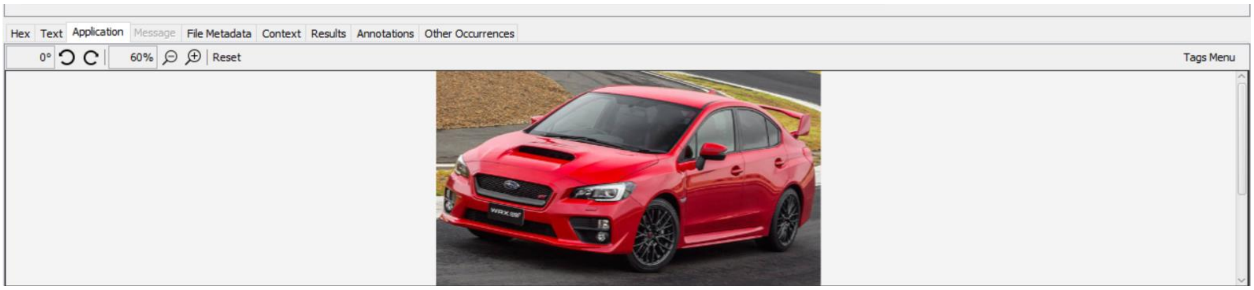


Figure 100: Extracted evidence car picture from HDD image 2.

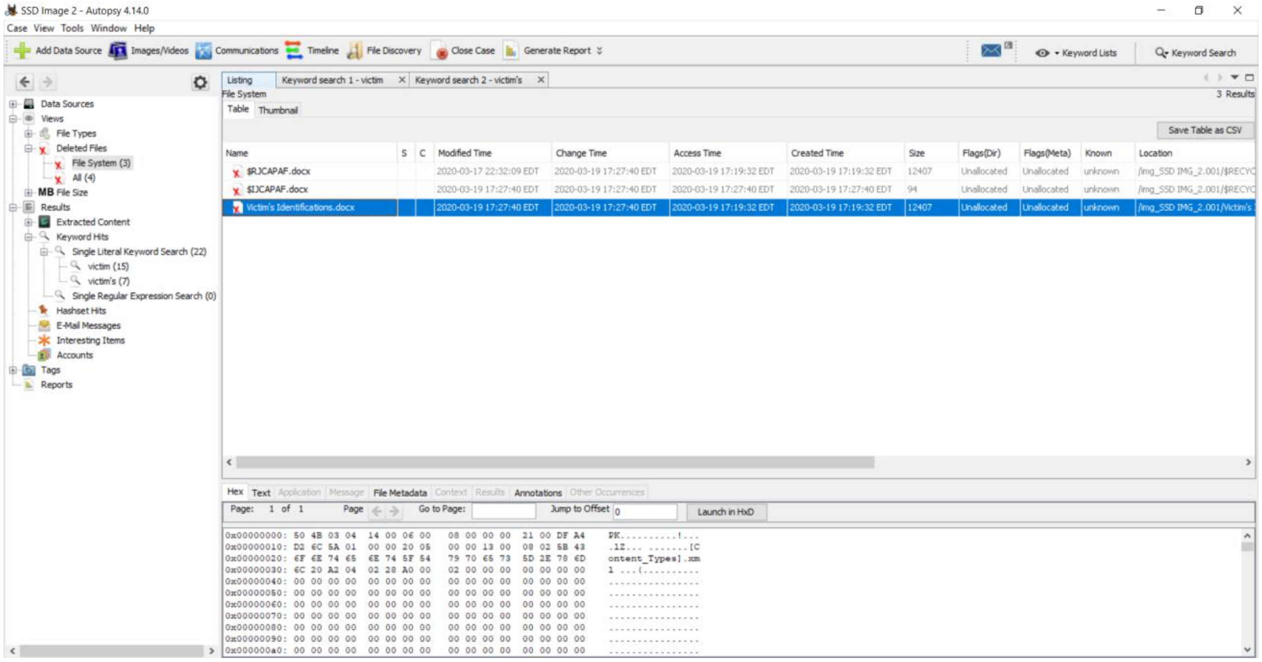
Table 5 below compares the total number of files in HDD before and after deleting evidence to the number of hits being generated when keywords are searched only for once.

Table 5

Comparing total files and keyword hits in HDD.

Keywords/Drive types	HDD before deleting		HDD after deleting	
	No. of files	No. of Hits	No. of files	No. of Hits
Victim's and victim	18	23	5	25

Similarly, SSD images 1 and 2 are loaded to Autopsy, and the results are analyzed (SSD Forensic Analysis, 2016). There was no big difference seen with the SSD image, as no files are deleted. The final report generated after analyzing is shown in figure 78 and searched for the same keywords as HDD. The keyword hits are noted for further comparison. The actual difference of this research study is observed in the SSD image 2. Here, after analyzing the SSD image 2, not all the deleted files were retrieved. The figure below shows that "victim's identifications.docx" is the only deleted from the SSD drive, but figure 48, shows all the deleted files. Only one file was retrieved out of 12 deleted files.



Name	S	C	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known	Location
$RJCAPAF.docx			2020-03-17 22:32:09 EDT	2020-03-19 17:27:40 EDT	2020-03-19 17:19:32 EDT	2020-03-19 17:19:32 EDT	12407	Unallocated	Unallocated	unknown	/img_SSD IMG_2.001/$RECYC
$IJCAPAF.docx			2020-03-19 17:27:40 EDT	2020-03-19 17:27:40 EDT	2020-03-19 17:27:40 EDT	2020-03-19 17:27:40 EDT	94	Unallocated	Unallocated	unknown	/img_SSD IMG_2.001/$RECYC
Victim's Identifications.docx			2020-03-19 17:27:40 EDT	2020-03-19 17:27:40 EDT	2020-03-19 17:19:32 EDT	2020-03-19 17:19:32 EDT	12407	Unallocated	Unallocated	unknown	/img_SSD IMG_2.001/Victim's

```
0x00000000: 50 4B 03 04  14 00 06 00  08 00 00 00  21 00 DF A4   PK..........!...
0x00000010: D2 6C 5A 01  00 00 20 05  00 00 13 00  08 02 5B 43   .lZ... .......[C
0x00000020: 6F 6E 74 65  6E 74 5F 54  79 70 65 73  5D 2E 78 6D   ontent_Types].xm
0x00000030: 6C 20 A2 04  02 28 A0 00  02 00 00 00  00 00 00 00   l ...(..........
0x00000040: 00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00   ................
0x00000050: 00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00   ................
0x00000060: 00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00   ................
0x00000070: 00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00   ................
0x00000080: 00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00   ................
0x00000090: 00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00   ................
0x000000a0: 00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00   ................
```

Figure 101: Deleted file retrieved from SSD image 2.

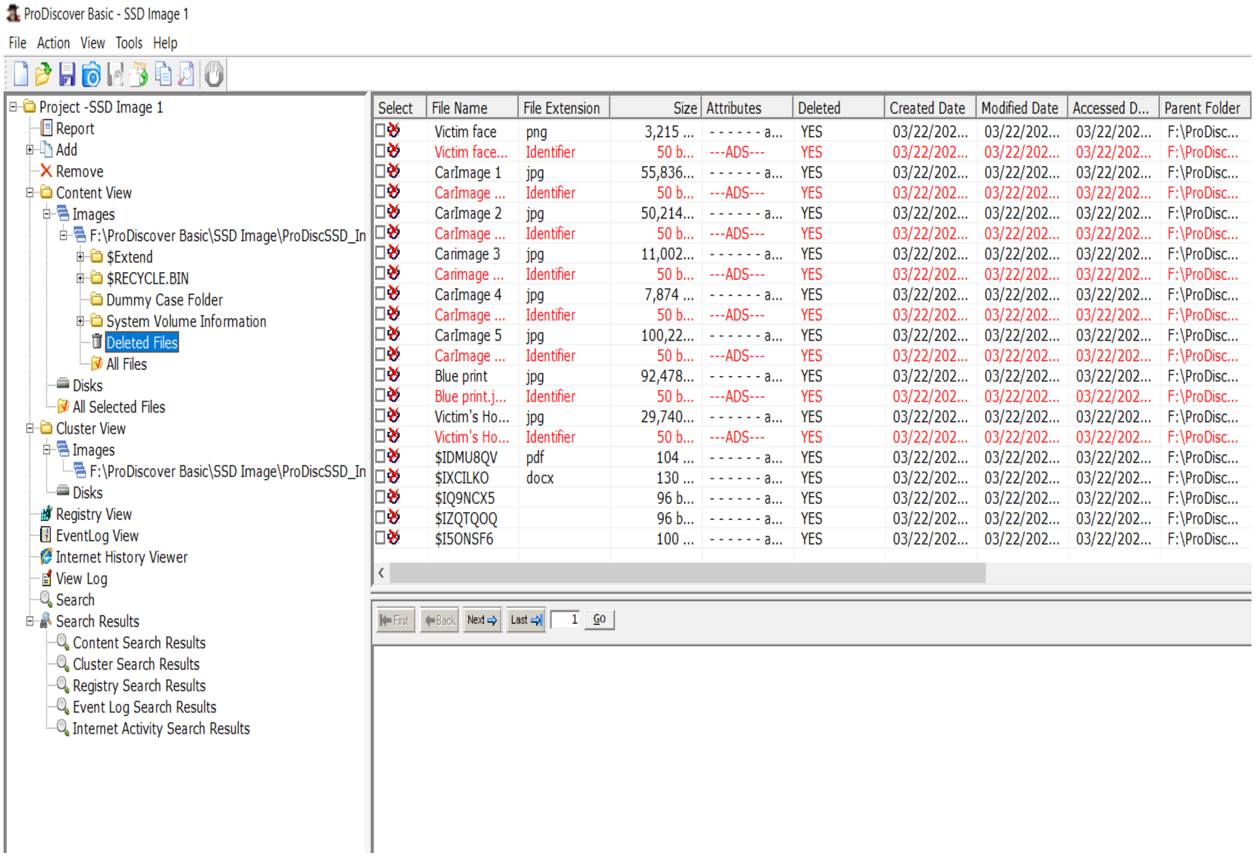
It is clear that deleted files in SSDs cannot be retrieved, whereas, in HDDs, deleted files can be retrieved. The keywords "victim" and "victim's" are searched in SSD image 2, and the number of keyword hits has been noted for comparison with the total number of files in below table 6.

Table 6:

Comparing total files and keyword hits from SSD.

Keywords/Drive types	SSD before deleting		SSD after deleting	
	No. of files	No. of Hits	No. of files	No. of Hits
Victim's and victim	18	32	5	22

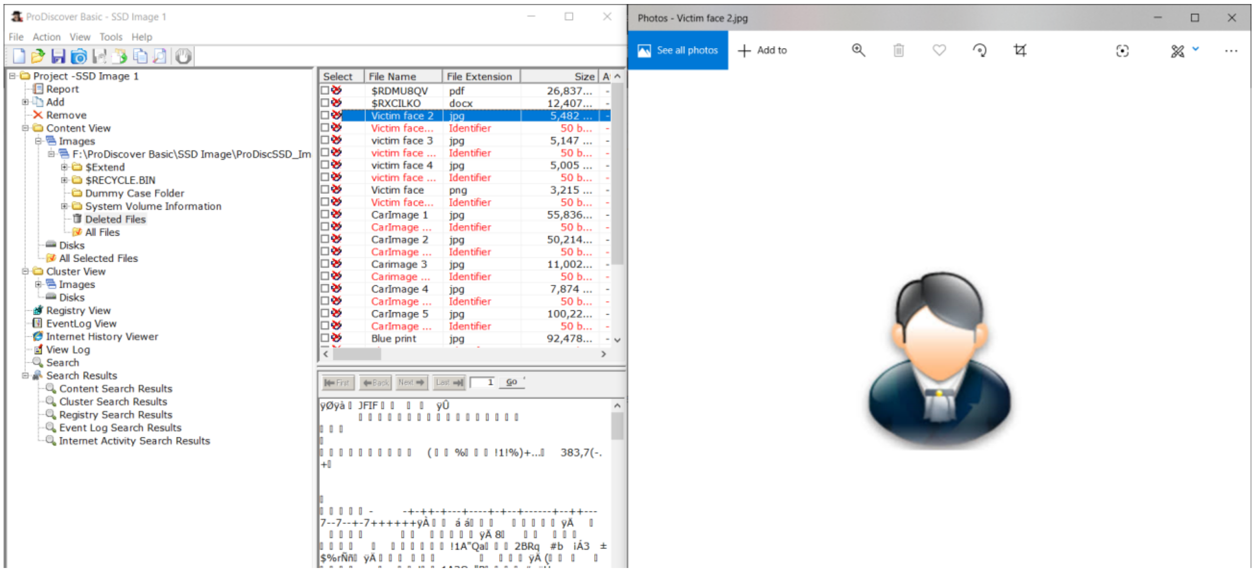
Now that it has been proved that files deleted from SSDs cannot completely be retrieved using Autopsy forensic tool, the other tool ProDiscover Basic has been used. "ProDiscSSD_Image.eve" image file is loaded to the tool, and the results obtained are shown below.



Select	File Name	File Extension	Size	Attributes	Deleted	Created Date	Modified Date	Accessed D...	Parent Folder
□	Victim face	png	3,215 ...	- - - - - - a...	YES	03/22/202...	03/22/202...	03/22/202...	F:\ProDisc...
□	Victim face...	Identifier	50 b...	---ADS---	YES	03/22/202...	03/22/202...	03/22/202...	F:\ProDisc...
□	CarImage 1	jpg	55,836...	- - - - - - a...	YES	03/22/202...	03/22/202...	03/22/202...	F:\ProDisc...
□	CarImage ...	Identifier	50 b...	---ADS---	YES	03/22/202...	03/22/202...	03/22/202...	F:\ProDisc...
□	CarImage 2	jpg	50,214...	- - - - - - a...	YES	03/22/202...	03/22/202...	03/22/202...	F:\ProDisc...
□	CarImage ...	Identifier	50 b...	---ADS---	YES	03/22/202...	03/22/202...	03/22/202...	F:\ProDisc...
□	Carimage 3	jpg	11,002...	- - - - - - a...	YES	03/22/202...	03/22/202...	03/22/202...	F:\ProDisc...
□	Carimage ...	Identifier	50 b...	---ADS---	YES	03/22/202...	03/22/202...	03/22/202...	F:\ProDisc...
□	CarImage 4	jpg	7,874 ...	- - - - - - a...	YES	03/22/202...	03/22/202...	03/22/202...	F:\ProDisc...
□	CarImage ...	Identifier	50 b...	---ADS---	YES	03/22/202...	03/22/202...	03/22/202...	F:\ProDisc...
□	CarImage 5	jpg	100,22...	- - - - - - a...	YES	03/22/202...	03/22/202...	03/22/202...	F:\ProDisc...
□	CarImage ...	Identifier	50 b...	---ADS---	YES	03/22/202...	03/22/202...	03/22/202...	F:\ProDisc...
□	Blue print	jpg	92,478...	- - - - - - a...	YES	03/22/202...	03/22/202...	03/22/202...	F:\ProDisc...
□	Blue print.j...	Identifier	50 b...	---ADS---	YES	03/22/202...	03/22/202...	03/22/202...	F:\ProDisc...
□	Victim's Ho...	jpg	29,740...	- - - - - - a...	YES	03/22/202...	03/22/202...	03/22/202...	F:\ProDisc...
□	Victim's Ho...	Identifier	50 b...	---ADS---	YES	03/22/202...	03/22/202...	03/22/202...	F:\ProDisc...
□	$IDMU8QV	pdf	104 ...	- - - - - - a...	YES	03/22/202...	03/22/202...	03/22/202...	F:\ProDisc...
□	$IXCILKO	docx	130 ...	- - - - - - a...	YES	03/22/202...	03/22/202...	03/22/202...	F:\ProDisc...
□	$IQ9NCX5		96 b...	- - - - - - a...	YES	03/22/202...	03/22/202...	03/22/202...	F:\ProDisc...
□	$IZQTQOQ		96 b...	- - - - - - a...	YES	03/22/202...	03/22/202...	03/22/202...	F:\ProDisc...
□	$I5ONSF6		100 ...	- - - - - - a...	YES	03/22/202...	03/22/202...	03/22/202...	F:\ProDisc...

Figure 102: Deleted files retrieved from SSD using ProDiscover Basic.

Figure 102 shows that all the deleted files on SSD can be retrieved. The same SSD image, when extracted using FTK Imager and analyzed in Autopsy, could not retrieve all the deleted files, whereas ProDiscover basic could retrieve all the deleted images. By this, it can be understood that drive images created using different tools show results differently when analyzed in different forensic tools. Even the deleted file content can be viewed using ProDiscover Basic, as shown in figure 103.



Select	File Name	File Extension	Size	A
□	$RDMU8QV	pdf	26,837...	-
□	$RXCILKO	docx	12,407...	-
□	Victim face 2	jpg	5,482 ...	-
□	Victim face...	Identifier	50 b...	-
□	victim face 3	jpg	5,147 ...	-
□	victim face ...	Identifier	50 b...	-
□	victim face 4	jpg	5,005 ...	-
□	victim face ...	Identifier	50 b...	-
□	Victim face	png	3,215 ...	-
□	Victim face...	Identifier	50 b...	-
□	CarImage 1	jpg	55,836...	-
□	CarImage ...	Identifier	50 b...	-
□	CarImage 2	jpg	50,214...	-
□	CarImage ...	Identifier	50 b...	-
□	Carimage 3	jpg	11,002...	-
□	Carimage ...	Identifier	50 b...	-
□	CarImage 4	jpg	7,874 ...	-
□	CarImage ...	Identifier	50 b...	-
□	CarImage 5	jpg	100,22...	-
□	CarImage ...	Identifier	50 b...	-
□	Blue print	jpg	92,478...	-

Figure 103: Deleted file content in the SSD image.

Conclusion

From the results obtained, this study concludes that data deleted on Hard Disk Drives can completely be retrieved, and data deleted on Solid-State Drives cannot be completely retrieved using Autopsy forensic tool, whereas sometimes it can be retrieved using ProDiscover Basic forensic tool. To understand this better, the data deleted on Hard drives are not completely wiped off. The Operating system has a pointer to each, and every file created and stored on a Hard drive. When a folder or file is deleted, it is just that the pointer is removed by the OS. This deleted data will still be present on the drive as long as new data is overwritten on these data sectors. Therefore, data deleted on Hard drives can be easily retrieved using forensic tools and data recovery tools.

When it comes to data deleted on SSDs it is totally different. Most of modern SSDs support TRIM. Deleted files on drives that have TRIM enabled cannot be retrieved. SSD read and write data from flash cells. Data on flash cells cannot be overwritten. Hence to write data, flash cells should be empty. As this study uses an external SSD, it is more likely that the TRIM command is disabled, resulting in not completely wiping the deleted files. The flash cells will not be wiped out if the TRIM command is disabled. In the case of an internal SSD, the TRIM is enabled by default, and OS immediately wipes out the deleted data to increase the write speed to SSD for any future use. The other property which makes it difficult to retrieve deleted data in self corrosion. SSDs have this property called self-corrosion. A process running in the background looks for unused data and wipes off flash cells permanently. So, when SSD image 2 is analyzed in Autopsy, deleted data might have undergone self-corrosion, and only one file was retrieved. Whereas, as this study used an external SSD, TRIM was disabled by default, and deleted data was retrieved using ProDiscover Basic. Thus, this study concludes, data deleted on SSDs is wiped out due to self-corrosion of SSD and disabled TRIM command, to improve the read/write performance speed time, which was lacked by traditional HDDs.

“If it takes one hour to write 10 GB data to your drive, it takes same time to wipeout, rather to save time Operating System removes the pointer and overwrites the deleted data sectors when needed.”

Future work

This study has proved that, SSDs behave differently when exposed to different forensic tools. Most of SSDs deleted data cannot be retrieved. This makes the job tough for the investigators and using SSDs become an advantage for criminals. No solution has been provided by this study. As a future work, finding solutions to this problem by enabling the TRIM command on external SSDs would be great and helps the investigators to retrieve the deleted data from SSDs.

References

(n.d.). Retrieved from MD5hashgenerator: https://www.md5hashgenerator.com/

Autopsy. (n.d.). Retrieved from Sleuthkit.org: https://www.sleuthkit.org/autopsy/

Ayusharma0698. (2018). Introduction to SSD's. Retrieved from geeksforgeeks: https://www.geeksforgeeks.org/introduction-to-solid-state-drive-ssd/

Balapure, A. (2018, May 19). Memory Forensics and Analysis Using Volatility. Retrieved from INFOSEC: https://resources.infosecinstitute.com/memory-forensics-and-analysis-using-volatility/#gref

Carrier, B. (2020). Autopsy. Retrieved from Sleuthkit: https://www.sleuthkit.org/autopsy/

Carroll, O., Brannon, S., & Song, T. (2017, September 12). Computer Forensics: Digital Forensic Analysis Methodology. Retrieved from crime scene investigator network: https://www.crime-scene-investigator.net/computer-forensics-digital-forensic-analysis-methodology.html#author

Casey, E. (2011). Digital Evidence and Computer Crime, Third Edition: Forensic Science, Computers, and the Internet. Watham, San Diego, London: Academic Press.

Chandel, R. (2015, September 29). Step by Step Tutorial of FTK Imager (Beginners Guide). Retrieved from Hacking Articles: https://www.hackingarticles.in/step-by-step-tutorial-of-ftk-imager-beginners-guide/

Cohen, P. (2016, November 17). A History of Hard Drives. Retrieved from BACKBLAZE: https://www.backblaze.com/blog/history-hard-drives/

Computer Forensic Examination Steps. . (n.d.). Retrieved from https://www.computer-forensics-recruiter.com/topics/examination_steps/#context/api/listings/prefilter

Definition of Encyclopedia. (n.d, n.d n.d). Retrieved from Encyclopedia: https://www.pcmag.com/encyclopedia/term/56084/solid-state-drive

Edwards, B. (2012, January 17). Evolution of the Solid-State Drive. Retrieved from PCWorld: https://www.pcworld.com/article/246617/evolution-of-the-solid-state-drive.html

Fahey, R. (n.d.). Computer Forensics: Forensic Analysis And Examination Planning. Retrieved from INFOSEC: https://resources.infosecinstitute.com/category/computerforensics/introduction/areas-of-study/forensic-science/forensic-analysis-and-examination-planning/#gref

Flash memory NAND NOR. (n.d.). Retrieved from Web.njit.edu: https://web.njit.edu/~rlopes/Mod8.3.pdf

Garfinkel, S. L. (2017, September 19). Digital forensics. Retrieved from American Scientist: https://www.americanscientist.org/article/digital-forensics

Geier, F. (2015). The differences between SSD and HDD technology regarding forensic investigations. Retrieved from gti.bh: http://www.gti.bh/Library/assets/fulltext01-gshhsy652.pdf

Grossi, D. (n.d.). What is Forensic science? - Definition, History & Types. Retrieved from study.com: https://study.com/academy/lesson/what-is-forensic-science-definition-history-types.html

Harrell, C. (2010, October 19). Overall DF Investigation Process. Retrieved from Journey Into the Incident Response : http://journeyintoir.blogspot.com/2010/10/overall-df-investigation-process.html

Lee, R. (2014, March 23). SANS Digital Forensics and Incident Response Blog. Retrieved from SANS Digital Forensic & Incident Response: https://digital-forensics.sans.org/blog/2014/03/23/sans-sift-3-0-virtual-machine-released/

Mark Reith Clint, M. R. (2002). An Examination of Digital Forensic Models . International Journal of Digital Evidence, Vol. 1, No. 3.

Morton, T. (2015, December 9). Introduction to Digital Forensics. Retrieved from wikibooks: https://en.wikibooks.org/wiki/Introduction_to_Digital_Forensics/Introduction

N.D. (2019, December 18). Forensic Toolkit. Retrieved from Wikipedia: https://en.wikipedia.org/wiki/Forensic_Toolkit

Nield, D. (2018, August 18). SSD vs HDD: What's the difference between flash storage and traditional hard drives? Retrieved from pocket-lint: https://www.pocket-lint.com/laptops/news/145421-ssd-vs-hdd-what-s-the-difference-between-flash-storage-and-hard-drives

Palmer, G. (2001, August 7,8). A Road Map for Digital Forensic Research. Retrieved from dfrws.org: http://www.dfrws.org/sites/default/files/session-files/a_road_map_for_digital_forensic_research.pdf

Platter. (2017, April 26). Retrieved from computerhope: https://www.computerhope.com/jargon/p/platter.htm

Prahlow, J. A. (2010). Forensic Pathology for Police, Death Investigators, Attorneys, and Forensic Scientists. New york: Humana Press.

Price, P. S. (n.d.). Digtal forensics. Retrieved from OpenLearn: https://www.open.edu/openlearn/science-maths-technology/digital-forensics/content-section-4.2

R, Y. (n.d). HDD vs SSD. Retrieved from geeksforgeeks: https://www.geeksforgeeks.org/hdd-vs-ssd/

Romano, P. (2014, September 2014). The Development and History of Solid State Drives (SSDs). Retrieved from Symmetry Electronics: https://www.semiconductorstore.com/blog/2014/The-Development-and-History-of-Solid-State-Drives-SSDs/854/

Rouse, M. (2017, November). flash memory. Retrieved from SearchStorage: https://searchstorage.techtarget.com/definition/flash-memory

SIFT Workstation Download. (n.d.). Retrieved from SANS DFIR: https://digital-forensics.sans.org/community/downloads

SSD Forensic Analysis. (2016, June 21). Retrieved from Computer Forensics: https://www.computer-forensics-recruiter.com/ssd-forensic-analysis/

Stephens, B. (2016, February 5). What is Digital Forensics? Retrieved from interworks: https://interworks.com/blog/bstephens/2016/02/05/what-digital-forensics/

Tabona, A. (2018, July 10). Top 20 Free Digital Forensic Investigation Tools for SysAdmins. Retrieved from TechTalk: https://techtalk.gfi.com/top-20-free-digital-forensic-investigation-tools-for-sysadmins/

The evolution of hard disk drives. (2019). Retrieved from https://www.pcworld.idg.com.au/slideshow/372650/evolution-hard-disk-drives/

Valli, A. J. (2009). Building a Digital Forensic Laboratory Establishing and Managing a Successful Facility. Burlington: Elsevier, Inc.

Weibe, J. (2013, May 05). Forensic Insight into Solid State Drives. Retrieved from Forensicmag: https://www.forensicmag.com/article/2013/05/forensic-insight-solid-state-drives

What exactly is Forensics? (n.d). Retrieved from discover criminal justice: https://discovercriminaljustice.com/articles/beyond-forensic-science-the-different-types-of-forensics/#context/api/listings

What is Forensic science? (n.d.). Retrieved from American Academy of Forensic Science: https://www.aafs.org/home-page/students/choosing-a-career/what-is-forensic-science/

Yunus Yusoff, R. I. (June 2011). COMMON PHASES OF COMPUTER FORENSICS. International Journal of Computer Science & Information Technology (IJCSIT), Vol 3, No 3.