LONTAR KOMPUTER VOL. 9, NO. 3 DECEMBER 2018 **p-ISSN 2088-1541**
DOI : 10.24843/LKJITI.2018.v09.i03.p06 **e-ISSN 2541-5832**
Accredited B by RISTEKDIKTI Decree No. 51/E/KPT/2017

Experimental Investigation of Frozen Solid State Drive on Digital Evidence with Static Forensic Methods

Imam Riadi[a1], Rusydi Umar[b2], Imam Mahfudl Nasrulloh[c3]

[a]Department of Information System, Universitas Ahmad Dahlan
Jln. Prof. Dr. Soepomo, S.H. Janturan, Yogyakarta, Indonesia
[1]imam.riadi@is.uad.ac.id

[bc]Department of Informatics, Universitas Ahmad Dahlan
Jln. Prof. Dr. Soepomo, S.H. Janturan, Yogyakarta, Indonesia
[2]rusydi_umar@rocketmail.com
[3]mahfudz.mail@email.com (Corresponding author)

Abstract

The rapid development of computer technology in hardware, is currently developing non-volatile computer storage media Solid State Drive (SSD). SSD technology has a faster data access speed than Hard Disk and is currently starting to replace Hard Disk storage media. Freezing software on computer systems is often carried out by computer technicians, because it can save a computer maintenance costs due to errors, be exposed to computer viruses or malware. This software is used to prevent unwanted changes to the computer system, when the computer is restarted changes that occur in the computer system will not be stored on storage media. When this happens, what should be done by digital forensic investigators. This study discusses experimental forensic investigations on SSD media storage with frozen conditions or in this study said the frozen SSD. Frozen SSD is the condition of the drive that is locked so that there is no change in the computer system. Software used to lock and prevent changes such as Deep Freeze, Shadow Defender, Windows Steady State, and Toolwiz Time Freeze. Forensic research stages using methods NIST. The result shows that from comparative analysis conducted with Deep Freeze the results of the RecoverMyFile gives 76.38% and Autopsy gives 75,27%, while frozen condition with Shadow Defender the results of the RecoverMyFile gives 59.72% and Autopsy gives 74.44%. So the results of this study indicate the drive freezing software has an effect obtained can be an obstacle in the digital forensic process.

Keywords: *Forensic, Digital, Evidence, SSD, NIST*

1. Introduction

Today's human activities are mostly related to data, information, and communication, and in their activities directly or indirectly will relate to computer technology devices. The use of everyday computer technology basically has enormous benefits, as the impact of computer use has positive benefits and negative impacts. The positive benefits of computer technology are very useful, so that it can help the process of difficult work to be easy and help human activities become easier, faster, and more efficient. The negative impact of computer technology is the abuse of computer technology used for crime, so that it can cause harm. Computer crime is a crime involving computer technology. Computer crime has electronic evidence and digital evidence in the form of traces of criminal activity and it is necessary to analyze digital evidence obtained by the forensic method [1]. In a case of computer technology crimes that occur in general will leave a trail of criminal activity. The history related to the crime can be used as evidence. Proof of computer crime can be in the form of electronic evidence and digital evidence [2]. Electronic evidence can be in the form of the physical form of the electronic device or can be in the form of storage media (storage device), while the digital evidence can be in the form of document files, history files, or log files that can be used as information supporting decision makers. Electronic evidence and digital evidence become the most important things in a computer crime case, because computer crime activities are recorded by a computer system on the main computer storage media.

There are two types of storage media on computers that are non-volatile memory and volatile memory. Non-volatile memory allows stored data to not be lost even if the power supply is disconnected or does not depend on the electrical power supply, such as hard drive, Solid State Drive (SSD), Memory Card, Zip Drive, Optical Drive, and Flash Disk, while the media Volatile Memory storage will lose data when the power is disconnected or there is no power supply, such as Random Access Memory (RAM), Dynamic Random Access Memory (DRAM), and Static Random Access Memory (SRAM) [3]. Solid State Drive (SSD) is a data storage device that uses a series of integrated circuits as the memory used to store data [4]. Solid State Drive (SSD) is one of the main storage media other than Hard disk. Solid State Drive (SSD) technology uses solid state memory based on NAND flash or NOR flash on the data storage, physically the difference between SSD and Hard disk (HDD) is on an SSD using a semiconductor or Integrated Circuit (IC) [5], while on a Hard disk using a rotating magnetic platter, is shown in Figure 1.

Figure 1. Solid State Drive (SSD)

This statistic depicts the suppliers' global market share of solid-state drive (SSD) unit shipments in the 4th quarter of 2014 in the second quarter of 2018. The total number of shipping units in the first quarter of 2018 was 45.46 million units. That quarter, Samsung had a market share, by units shipped, by 32.2 percent [6]. From the data supplier then currently the SSD is gradually replacing the hard drive position on the main computer storage media, because this SSD technology has high data access speeds compared to hard drives.

In general, computer technicians to save maintenance costs and maintenance time do tricks using utility software to freeze the system on the computer, including freezing the drive to be safe from unwanted changes. Some software freezes computer systems and drives on computers, such software as Deep Freeze, Shadow Defender, Windows Steady State, and Toolwiz Time Freeze. This software has a system recovery feature and freezing the drives on computer storage media. When the settings in the software are activated, changes to the computer system will not be stored in the storage media. The software system works when the computer is turned off and turned on so the state of the computer system is like before changes are made, as well as when storing a file on a frozen drive then the storage space conditions will return as before the file was saved.

A Deep Freeze software developer on his website deepfreeze.com.au says software to freeze drives can reduce computer maintenance costs, so as to save on maintenance costs for offices and internet cafes, in Indonesia offices and internet cafes use this application. Also said on the website of software developer Shadow Defender, the application will take a snapshot of the disk and run each file in virtual mode, after the user exits from a parallel dimension any changes to the system and files on the disk will be deleted. In detail the way Deep Freeze works on the drive is when the computer is turned on and the drive is used, it will make the allocation of the table in the file system in an empty block, but when the computer is restarted the filled block will become empty again [7], and this condition can be said to be anti-forensics, a technique to complicate the computer forensic process [8], as shown in Figure 2.

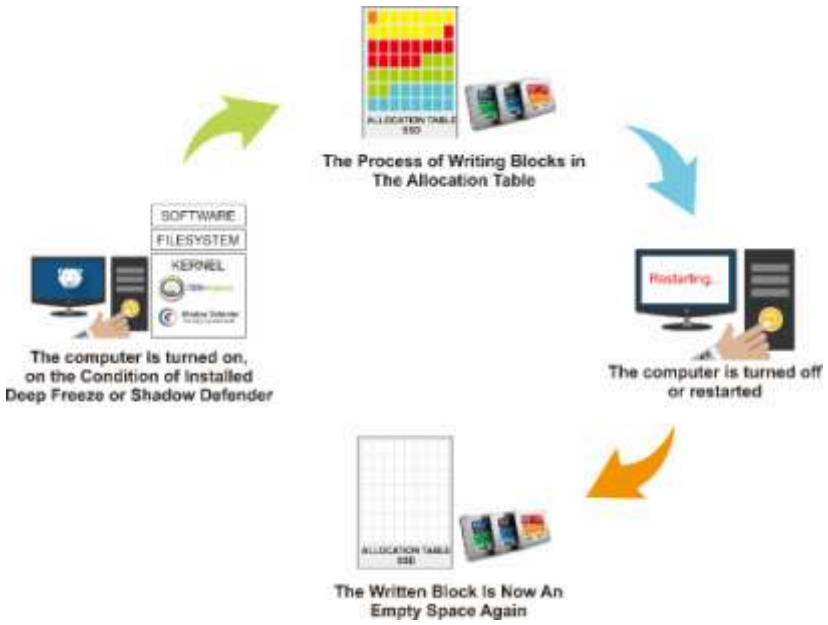

Figure 2. How to Work Deep Freeze or Shadow Defender

Previous research has been done [7] he did it on the hard disk storage media, all activities to be written on the hard drive partitions which were frozen by Deepfreeze software (frozen hard drive) will be returned when the computer restarting or shutdown. That could be difficult to find digital evidence in a crime if frozen hard drive has been installed on the computer (evidence) because the digital evidence will be lost when the computer is off. In the case of other studies [9], a comparison of forensic analysis on the HDD hard drive) and solid state drive (SSD) has been compared under standard conditions. The results of the study showed different results both. Therefore, this research was carried out and applied to solid state drive (SSD) storage media but was frozen with Deep Freeze and Shadow Devender software, and then compared the results of both which had influence on obtaining digital evidence.

Basically, a Solid state drive (SSD) is the same as a Hard disk (HDD). It's just that Solid state drives don't have magnetic layers such as a Hard disk. Solid state drives store all data on a flash memory chip that is interconnected, while the Hard disk is composed of mechanical and electronic components. Mechanical parts the Hard disk consists of a motor and an arm connected to a disk. The process of writing and reading data is done through a mechanical process in which the disk is rotated by the motor and the end of the arm connected to the electronic component that processes and performs the writing and reading of data on the disk. In general, Hard disk data processing is carried out because of the synergy between mechanical and electrical activities [3]. Solid state drives in processing data, writing and reading data are not supported by mechanical processes. In Solid state drives there are only electronic components such as Integrated Circuit or IC, microchip and other supporting electronic components such as capacitors. All the process of reading and writing data is done electrically just like the process that occurs in the Flash Disk and RAM memory [9]. Because of its spiral shape, Hard disk stores files located on adjacent blocks, when Hard disk capacity starts to be full of files that have been stored it can be scattered or known as fragmentation. The effect of fragmentation is the decrease in performance of the Hard disk. Whereas there is no fragmentation of the Solid state drive because the data is stored on a flash chip.

The condition of a computer using an Solid sate drive (SSD) and in a frozen drive condition is a challenge for digital forensic investigators. Required to experiment forensic analysis of digital evidence on the condition of frozen solid state drives. This challenges computer forensic investigators and how to analyze digital evidence in the above conditions if it occurs on a solid state disk (SSD). The frozen condition on a solid state disk (SSD) drive is the condition of a locked drive so that there are no changes in the computer system. In computer systems installed

utility software that is used to protect computers from unwanted changes. The freezing drive software used in this study is Shadow Defender and Deep Freeze.

2. Research Methods

Forensic analysis of digital or electronic evidence is referred to as forensic or digital forensic computers [10]. Digital forensics is an act of obtaining, retrieving, preserving, and presenting data in accordance with forensic methods and tools. Investigation of digital crime is very necessary to assist the process of an investigation [11]. Likewise, digital evidence analysis needs to be carried out in accordance with specific handling procedures and appropriate methods of forensic analysis, to obtain good digital evidence, so that from the digital evidence obtained evidence in the form of valid information to support the legal decision of a case of computer crime [12], [13].

Forensic analysis implements methods from the National Institute of Standards and Technology (NIST) with forensic stages of Collection, Examination, Analysis and Reporting [14], [15]. This method of forensic analysis from the National Institute of Standards and Technology (NIST) is to explain how the stages of forensic analysis will be carried out, so that it can know the flow and steps of the research systematically so that it can be used as a guide in solving existing problems [16]. Conducting forensic techniques and forensic analysis based on the correct method will have high success in collecting forensic data [17]. The stages in this study adopted and implemented the National Institute of Standards and Technology (NIST), as shown in Figure 3.

Figure 3. National Institute of Standards and Technology (NIST) Method

Stages from the NIST method are divided into four stages, namely Collecting, Examination, Analysis, and Reporting [14][15]. The complete description is as follows:

a. Collection

   Collection stage is a series of activities to collect data to support the investigative process in order to find evidence of digital crime. At this stage there is a process of retrieving data from relevant data sources and maintaining the integrity of evidence from changes.

b. Examination

   The examination stage is the stage of checking forensic data collected either automatically or manually, and ensuring that the data obtained in the form of the original file is in accordance with that obtained at the scene of computer crime, for that the digital file needs identification and validation. file with hashing technique.

c. Analysis

   The analysis stage is done after getting the desired digital file or data from the previous inspection process, then the data is analyzed in detail and comprehensively with a technically and legally justified method to be able to prove the data. The results of the analysis of digital data are hereinafter referred to as digital evidence and can be accounted for scientifically and legally.

d. Reporting

   The reporting stage is an activity carried out after the digital evidence is examined and analyzed. At this stage the reporting includes a description of the actions taken, an explanation of the tools, and the methods used, determining the actions taken, and providing recommendations for policy makers, methods, tools, or other supporting aspects during the digital forensic process.

Static forensics refers to traditional forensic investigations carried out with the device not active or not working [7]. Static forensics focuses on examining duplicate copies of storage media to retrieve existing data, for example, such as deleted files, website history, user history, and computer log history [13]. Copies of evidence can be obtained using various types of external storage media devices such as USB Flash disks, External Hard Drives, and other storage

media. Furthermore, copies of digital evidence are taken to the forensic laboratory by investigators to analyze data for verification [2]. In this research digital evidence used is not obtained from the results of actual computer crime, but digital evidence is made and obtained from the results of case scenarios and implementation of tests which will be discussed in a separate sub-section. This research phase refers to the four stages of the National Institute of Standards and Technology (NIST) and this research step is divided into four main sections, as in Figure 4.

Figure 4. Flowchart of Research Stages

In support of this experiment a forensic tool is needed both hardware and software. These tools are as shown in Table 1.

Table 1. Tool for Experimental Investigation

No	Experiment Tools	Description
1	SSD Samsung 120GB	Samsung EVO 850 MZ-75E120
2	SSD Transcend 128GB	Transcend SSD360 TS128GSSD360S
3	Tableau Forensic SATA/IDE Bridge	T35u-RW Series
4	Notebook	Acer Z1402, OS Windows 10 64 bit
5	Computer Desktop	Proc Intel G3220, 8GB RAM, HDD 1TB
6	Deep Freeze 8.20	Applications used for frozen drives SSD
7	Shadow Defender 1.4	Applications used for frozen drives SSD

Forensic tools used by researchers for the process of forensic analysis, extraction, and digital file restoration, as in Table 2.

Table 2. Forensics Tools

No	Forensics Tools	Description
1	Tableau Imager 1.2	Proprietary applications used to make acquisition of evidence such as a storage device
2	Autopsy 4.8	Open Source Applications that can be used to acquire digital evidence from multiple sources
3	Encase 7.10	Proprietary applications used to obtain digital evidence on storage devices
4	FTK Imager 3.4	Proprietary applications used to obtain digital evidence on storage devices
5	RecoverMyFile 5	Proprietary applications used to obtain digital evidence on storage devices
6	OSForensics 3.3	Proprietary applications used to obtain digital evidence on storage devices

3. Result and Discussion

In the results section and this discussion in full the stages of the research carried out are explained. As in the previous section this study has four stages. This section will discuss the results obtained at each stage.

3.1. Results from Stages Case Scenario and Implementation

The results at the scenario implementation stage are aimed at obtaining digital evidence as in the case of actual computer crime, then scenarios are as follows:

a. Preparing a computer that will be used for experiments, on the computer the main storage media used is the solid state drive (SSD).
b. Turn on the computer and activate the drive freezing feature in the Deep Freeze and Shadow Defender software, as in Figure 5.
c. Open file, edit the file, and save file on the frozen drive condition. In this experiment each file type is prepared, there are 360 files of different types. The file type is a document file (eg.doc, .xls, .ppt, .pdf), image file (eg .jpg, .bmp .png), multimedia files (eg .mp3, .mp4), archive files (eg .rar, .zip), and application files (eg .exe). At this stage computer crime scenarios are designed, computer criminals edit files and modify files.
d. Copy files from a frozen drive via flash disk and copy files to frozen drive.
e. The computer is turned off as if the computer has been used for computer crime.

When turned off the logic of the file has been lost, because in the computer system is activated frozen drive on a solid state drive (SSD) with Deep Freeze and Shadow Defender software. Users will think the file has been deleted, so in this experiment the researcher will prove whether the file still exists or the file is deleted cannot be returned.

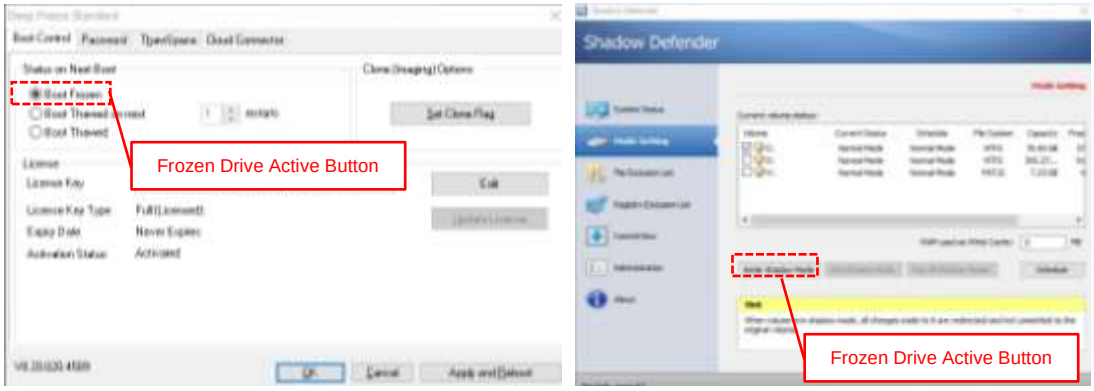

Figure 5. Display in Deep Freeze and Shadow Defender to Activate Frozen Drive

In the next step, electronic evidence in the form of a computer obtained from the scene is secured and then a solid state drive is taken to make a copy. The acquisition process aims to get the original copy to be analyzed and extracted to obtain digital evidence. Original evidence is stored and reopened in court if necessary.

3.2. Results from Stages Digital Evidence Acquisition

This stage is the acquisition stage, acquisition is taking a copy of the original. At this stage using the The results of the acquisition using the tool have the DD format. The DD file format is also referred to as the raw image type. This is a copy of data from the media save by byte by byte without having to be formulated [13]. Copy size and copied disk are the same. Additionally DD files do not store metadata from copies. The file extension is DD (RAW). The tool used for acquisition, as in Figure 6.

Tableau Forensic SATA/IDE Bridge acquisition tool and the Tableau Imager (TIM) software. The imaging results of the Samsung 850 SSD Evo 120GB drive show the size of 120,034,123,776 bytes and Transcend SSD360S 128GB drive shows 128,035,676,160 bytes.

Figure 6. Tableau Forensic SATA/IDE Bridge and Computer Examiner

The acquisition, image file includes a hash value, the hash value is used to equalize the similarities of large computer files. So forensic investigators use it to compare original acquisition files with duplicate files. The hash value generated by the acquisition tool as in Figure 7.

Figure 7. Hash Value of Original Image Acquisition File

After the acquisition file is made in the form of an image drive, then the process of checking and analyzing must be made a copy of the image. In order for file acquisition integrity to be maintained. After copying it is necessary to have hashed and compare the hash (checksum) value of the original acquisition file with the file that will be used forensic analysis, both must have the same hash value as in Figure 8.

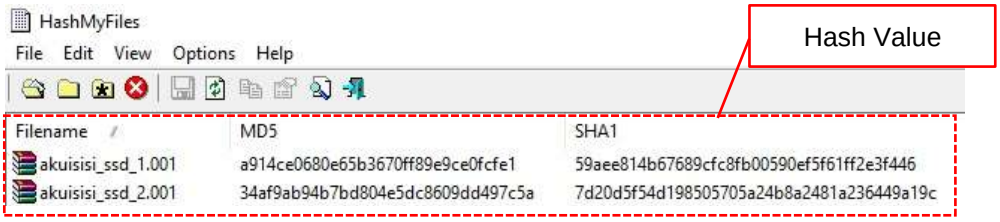

Figure 8. Hash Value of Duplicate Image Acquisition File

After checking the authenticity of both the original image file and the copy image, the next step is to examine and analyze the data on the copy of the drive to obtain digital evidence or evidence related to computer crime.

3.3. Results from Stages Digital Evidence Forensic Analysis

This section explains the results of research on forensic analysis of digital evidence on frozen solid state drives (SSD). The tools used to analyze are RecoverMyFile, Autopsy, FTK, Encase, and OSForensics [18]. In principle, forensic tools are the same, used to open directory structures and data structures. The results of frozen solid state drives (SSD) using the RecoverMyFile forensic tool, directory structures and artifact files can be seen and get the results of the files tested in this experiment. The results of the analysis and obtaining artifacts are shown in Figure 9.

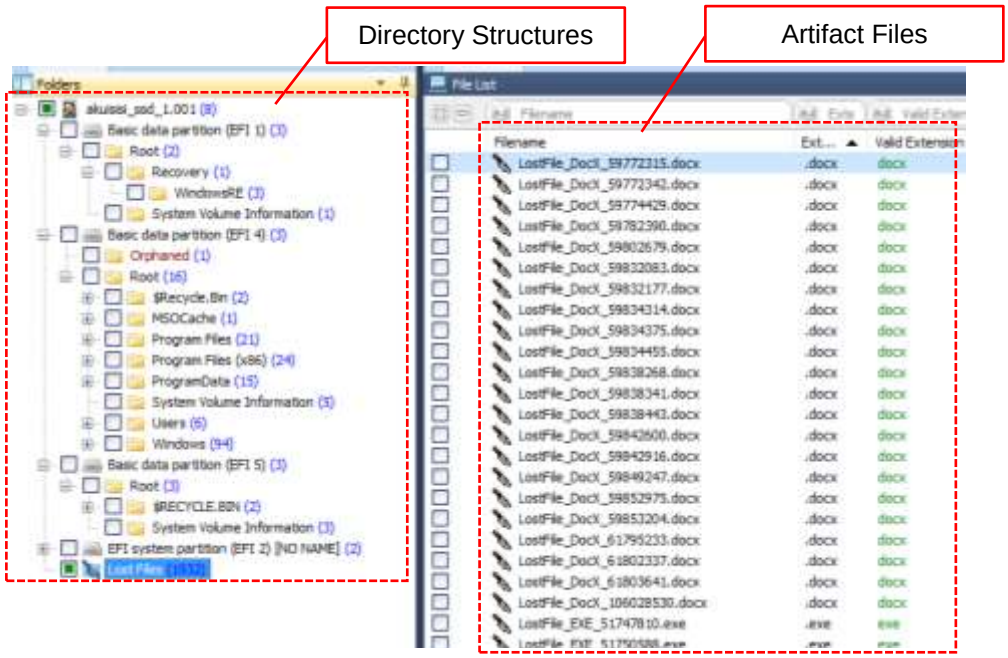

Figure 9. Examination Process on RecoverMyFile

Analyze uses the Autopsy-The Sleuth Kit can be seen in the directory structure and artifact files. Using this tool is the file that was tested in this experiment. The results of the analysis and obtaining artifacts are shown in Figure 10.

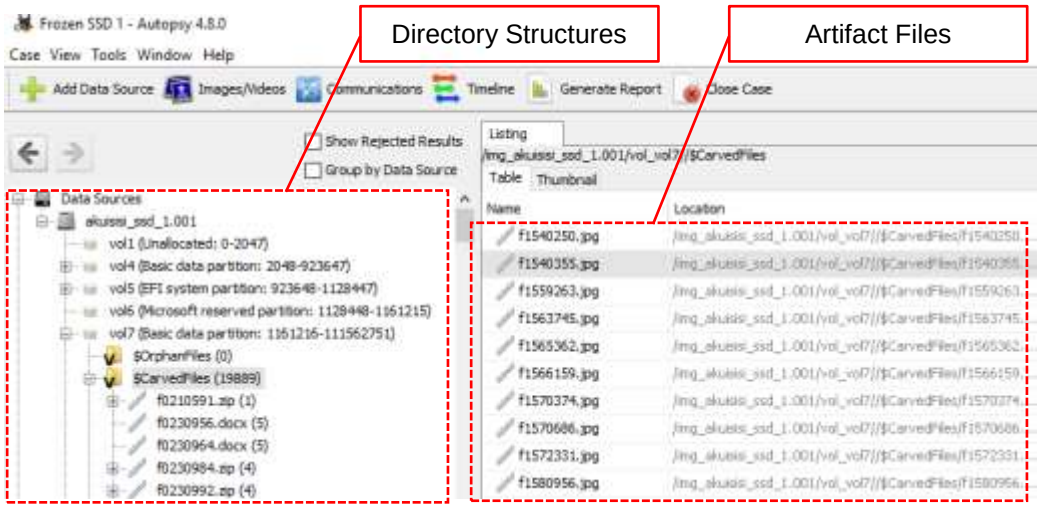

Figure 10. Examination Process on The Sleuth Kit Autopsy

Forensic analysis results using Encase forensic tools, can be seen in the directory structure and artifact files, but no files were tested in this experiment. The results of the analysis and obtaining artifacts are shown in Figure 11.

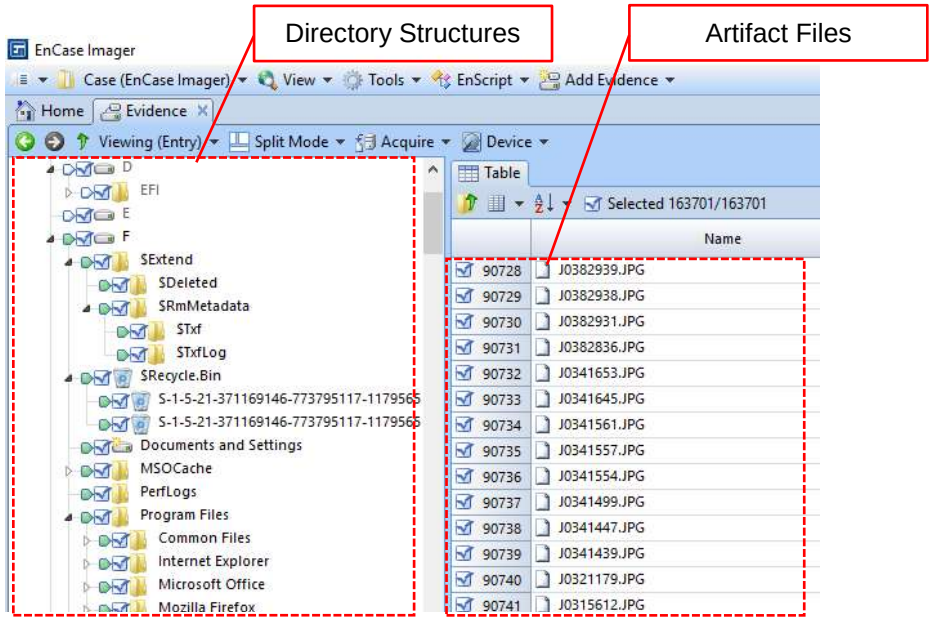

Figure 11. Examination Process on Encase

The results of the next forensic analysis using FTK forensic tools, can be seen in the directory structure and artifact files but no files were tested in this experiment. The results of the analysis and obtaining artifacts are shown in Figure 12.

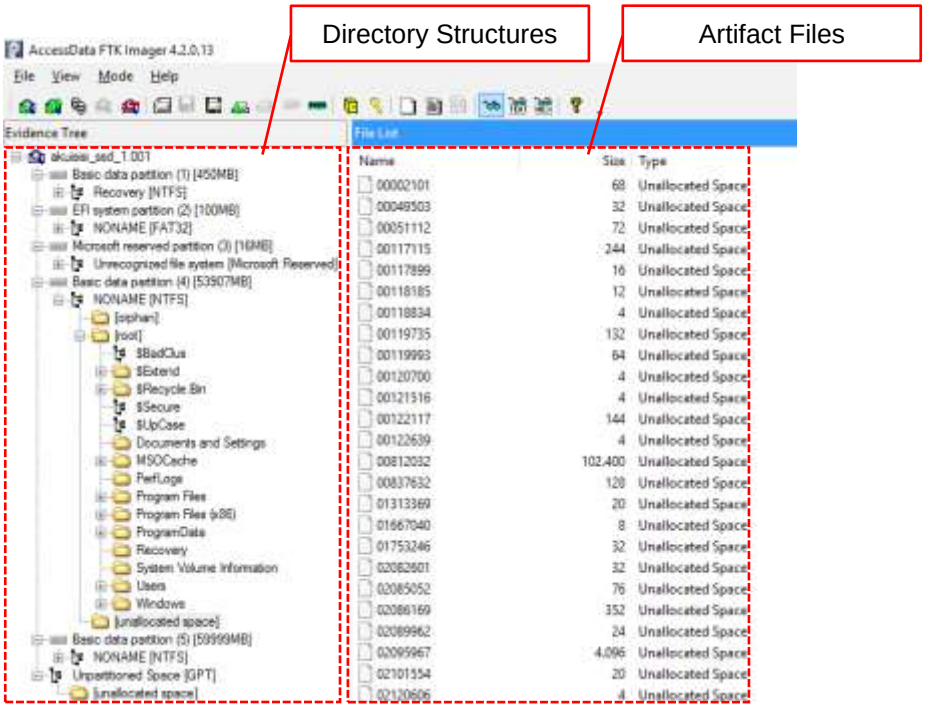

Figure 12. Examination Process on FTK Imager

The results of the last forensic analysis using OSForensics forensic tools, using this tool can only be seen in the directory structure. There are no files found in this experiment, shown in Figure 13.

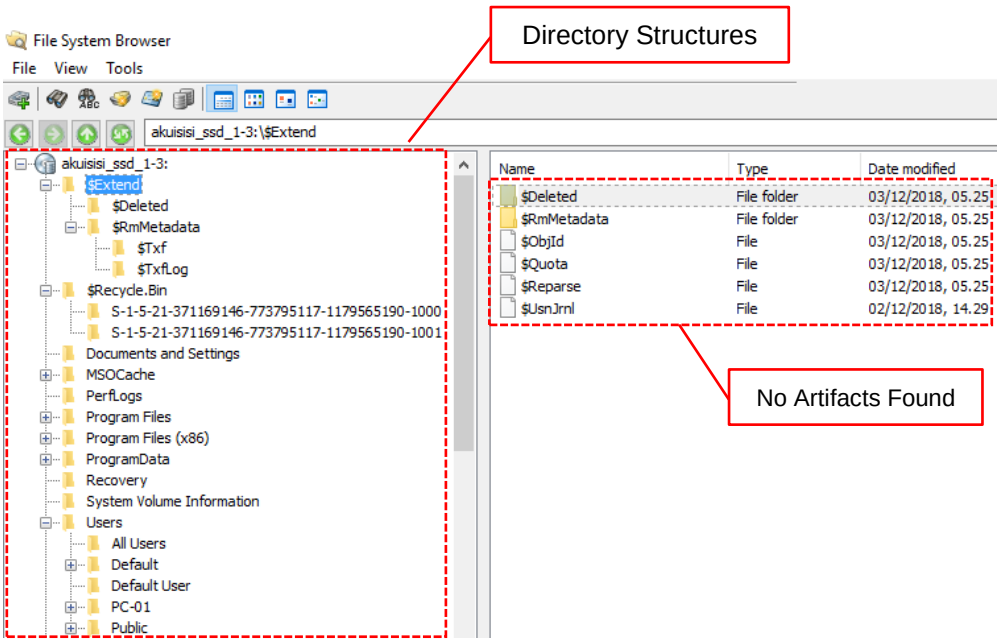

Figure 13. Examination Process on OSForensics

The results of forensic analysis with various forensic tools show that not all tools can read artifacts and there are two tools that can read artifacts with significant results are RecoverMyFile and Autopsy-The Sleuth Kit. From the forensic tool extraction is done to the original file, but not all can be extracted and restored probably because the data structure of the file has been corrupted so that the returned file is not perfect. The results of artifacts files that can be extracted in the form of the original file as in Figure 14.

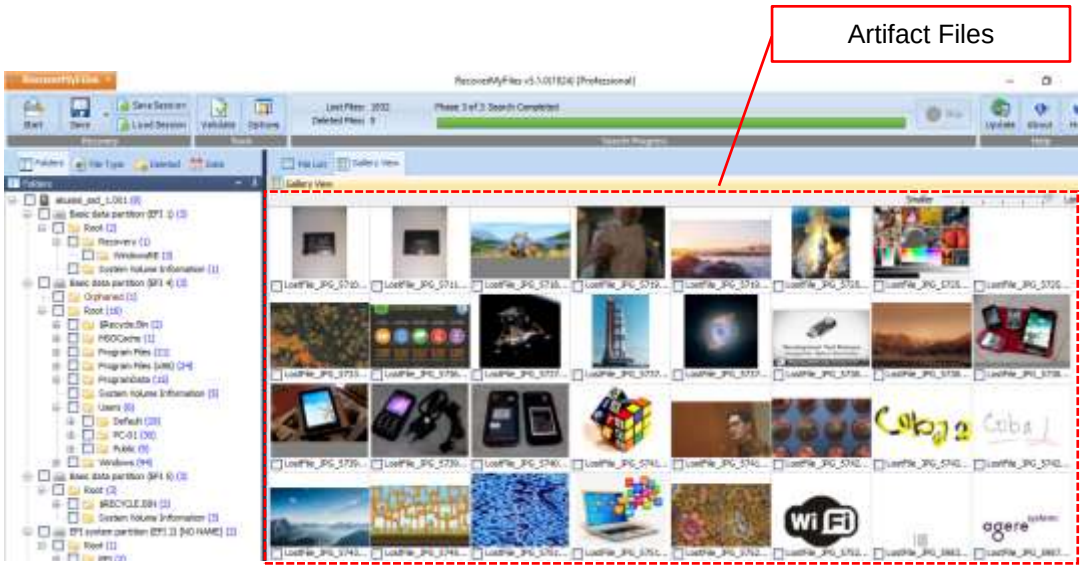

Figure 14. Artifact Files Viewed with RecoverMyFile

From the extraction of artifact files, export to the original file format using the forensic tools used. In general, forensic tools provide menus for exporting to file formats. As said before, not all artifact files can be extracted, as in Figure 15.

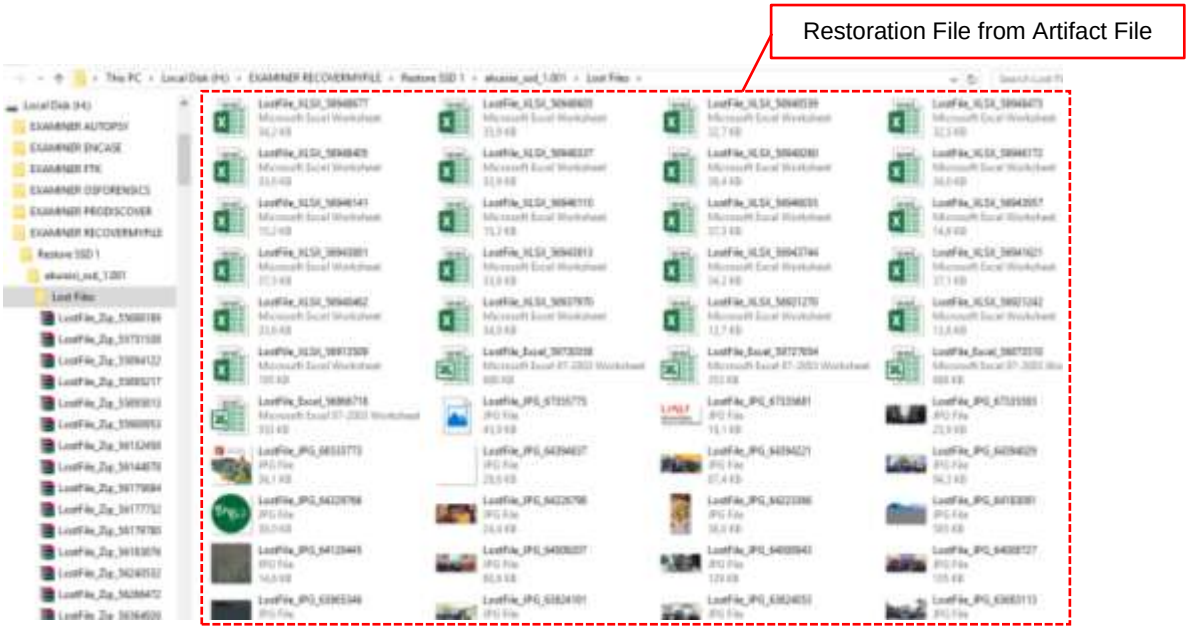

Figure 15. Export Files from the Forensic Tool

3.4. Result from Stages of Digital Evidence Reporting

The final stage in the NIST forensic method is reporting. At this stage all the results of the analysis will be presented in detail and all the results of the analysis related to the performance comparison of forensic devices obtained from frozen solid state drives (SSD) are documented. Reports are presented in the form of comparison tables based on the results of artifacts and the results of restoration of digital evidence. In Table 3 digital evidence obtained from frozen solid state drives (SSD) with Deep Freeze.

Table 3. Restoreable Files from Frozen SSD with Deep Freeze

File Type	Forensic Tools				
	RecoverMyFile	Autopsy	FTK	Encase	OSForensics
Document file					
.doc	18	30	0	0	0
.xls	19	23	0	0	0
.ppt	14	20	0	0	0
.pdf	20	22	0	0	0
Image file					
.jpg	30	30	0	0	0
.bmp	21	24	0	0	0
.png	30	16	0	0	0
Multimedia file					
.mp3	30	19	0	0	0
.mp4	20	25	0	0	0
Archive file					
.rar	18	6	0	0	0
.zip	30	30	0	0	0
Application file					
.exe	25	26	0	0	0

The results obtained from the five forensic devices used for a frozen solid state drive (SSD) examination with Shadow Defender freezing software has two tools whose results are very good, namely RecoverMyFile and Autopsy. The forensic tool can restore almost all the files that are tested. Unlike the other three forensic tools, the performance of the tool can show the file directory but cannot show artifact files. So that this experiment does not show the results obtained. The next experimental results can be seen in Table 4, results are obtained on the frozen solid state drive (SSD) with Shadow Defender freezing software.

Table 4. Restoreable Files from Frozen SSD with Shadow Defender

File Type	Forensic Tools				
	RecoverMyFile	Autopsy	FTK	Encase	OSForensics
Document file					
.doc	20	25	0	0	0
.xls	19	23	0	0	0
.ppt	5	20	0	0	0
.pdf	30	22	0	0	0
Image file					
.jpg	30	30	0	0	0
.bmp	0	26	0	0	0
.png	0	30	0	0	0
Multimedia file					
.mp3	30	19	0	0	0
.mp4	0	26	0	0	0
Archive file					
.rar	27	30	0	0	0
.zip	30	16	0	0	0
Application file					
.exe	24	29	0	0	0

In the table shows the results of the five forensic tools used, the results obtained in the examination process, there are two forensic tools whose results are very significant, namely RecoverMyFile and The Sleuth Kit Autopsy. But the results obtained differ on the frozen solid state drive (SSD) with Deep Freeze compared to Shadow Defender. Determining the performance of the forensic tools used and against digital evidence obtained from the examination process, researchers used the calculation of index numbers. The index number calculation used is unweighted index, as shown in Equation (1).

$$Eon = \frac{\sum En}{\sum Eo} \times 100\% \quad (1)$$

In the equation, $\sum En$ is digital evidence obtained, $\sum Eo$ is the number of experimental samples prepared as evidence, and Eon is the value of the evidence obtained. The results of the index number calculation from the performance of the forensic tools used and the drive freezing software that are implemented, show the results as in Table 5.

Table 5. Performance Forensic Tools for Digital Evidence

Freezing Software	Forensic Tools				
	RecoverMyFile	Autopsy	FTK	Encase	OSForensics
Deep Freeze	76,38%	75,27%	0%	0%	0%
Shadow Defender	59.72%	74,44%	0%	0%	0%

4. Conclusion

On a computer that uses a Solid state drive (SSD) or Hard disk (HDD), and in a frozen state Solid state drive and on a hard disk in a frozen condition, forensic processes can be done even though they have different ways of working. Based on experimental results the use of frozen software and using various forensic tools for the extraction and examination processes. Can be concluded that not all files can be recovered properly because the file structure and data are damaged. Not all artifacts can be read by all forensic devices, only some forensic devices show significant results. From the experimental results obtained index values based on the ability of the forensic tool in finding and restoring files, with RecoverMyFile obtained an index value of 76,38%, Autopsy has an index value of 75,27%, FTK has an index value of 0%, Encase has an index value of 0%, and OSForensics has an index value of 0% obtained from 360 files tested with freezing conditions with Deep Freeze software. While in frozen conditions with Shadow Defender software, RecoverMyFile has a number index of 59,72%, Autopsy has an index of 74,44%, FTK has an index value of 0%, Encase has an index value of 0%, and OSForensics has an index value of 0% obtained from 360 files tested. So that it can become an obstacle in the digital forensic process by investigators, and the results of the investigation are still very little

information obtained from digital evidence. Based on information obtained from investigations, experiments, and reference literature implemented in this study, it is evident that frozen solid state drive (SSD) mechanisms can inhibit digital forensic investigations. This mechanism has an effect on the operating system that is running and the storage system on the computer.

References

[1] S. Vidwarshi and N. Chandra, "Analysis of Development Phases in Digital Forensics," *International Journal of Advanced Computational Engineering and Networking*, vol. 2, no. 8, pp. 90–95, 2015.

[2] R. Ruuhwan, I. Riadi, and Y. Prayudi, "Evaluation of Integrated Ddigital Forensics Investigation Framework for The Investigation of Smartphones Using Soft System Methodology," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 7, no. 5, pp. 2806–2817, 2017.

[3] A. Silberschatz, P. B. Galvin, and G. Gagne, *Operating System Concepts*, 9th ed. United States of America: John Wiley & Sons, Inc., 2013.

[4] F. Geier, "The Differences Between SSD and HDD Technology Regarding Forensic Investigations," Linnaeus University Sweden, 2015.

[5] R. A. Ramadhan, Y. Prayudi, and B. Sugiantoro, "Implementasi dan Analisis Forensika Digital pada Fitur Trim Solid State Drive (SSD)," *Teknomatika*, vol. 9, no. 2, pp. 1–13, 2017.

[6] Statista, "Solid-state Disk Drives (SSD) Share of Quarterly Share of Unit Shipments Worldwide from 2014 to 2018," *Statista.com*, 2015. [Online]. Available: https://www.statista.com/statistics/412158/global-market-share-solid-state-drive-suppliers/. [Accessed: 12-Aug-2018].

[7] F. Albanna and I. Riadi, "Forensic Analysis of Frozen Hard Drive Using Static Forensics Method," *International Journal of Computer Science and Information Security (IJCSIS)*, vol. 15, no. 1, pp. 173–178, 2017.

[8] B. Rahardjo and I. P. A. E. Pratama, "Pengujian Dan Analisa Anti Komputer Forensik Menggunakan Shred Tool," *Lontar Komputer : Jurnal Ilmiah Teknologi Informasi*, vol. 7, no. 2, pp. 104–114, 2016.

[9] S. S. R. Marupudi, "Solid State Drive : New Challenge for Forensic Investigation," St. Cloud State University, 2017.

[10] I. Riadi, S. Sunardi, and A. Fauzan, "Examination of Digital Evidence on Android-based LINE Messenger," *International Journal of Cyber-Security and Digital Forensics (IJCSDF)*, vol. 7, no. 3, pp. 337–343, 2018.

[11] I. Riadi, J. Eko, A. Ashari, and S. -, "Internet Forensics Framework Based-on Clustering," *International Journal of Advanced Computer Science and Applications (IJACSA)*, vol. 4, no. 12, pp. 115–123, 2013.

[12] F. Jafari and R. S. Satti, "Comparative Analysis of Digital Forensic Models," *Journal of Advances in Computer Networks*, vol. 3, no. 1, pp. 82–86, 2015.

[13] E. Akbal and S. Dogan, "Forensics Image Acquisition Process of Digital Evidence," *International Journal of Computer Network and Information Security*, vol. 10, no. 5, pp. 1–8, 2018.

[14] I. Riadi, R. Umar, and A. Firdonsyah, "Forensic Tools Performance Analysis on Android-based Blackberry Messenger using NIST Measurements," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 8, no. 5, pp. 3991–4003, 2018.

[15] R. Umar, I. Riadi, and G. M. Zamroni, "Mobile Forensic Tools Evaluation for Digital Crime Investigation," *International Journal on Advanced Science, Engineering and Information Technology (IJASEIT)*, vol. 8, no. 3, p. 949, 2018.

[16] R. Umar, A. Yudhana, and M. N. Faiz, "Experimental Analysis of Web Browser Sessions using Live Forensics Method," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 8, no. 5, pp. 2951–2958, 2018.

[17] I. Riadi and R. Umar, "Identification of Digital Evidence on Android's Blackberry Messenger Using NIST Mobile Forensic Method," *International Journal of Computer Science and Information Security (IJCSIS)*, vol. 15, no. 5, pp. 155–160, 2017.

[18] M. Patankar and D. Bhandari, "Forensic Tools used in Digital Crime Investigation," *Indian Journal of Applied Research*, vol. 4, no. 5, pp. 278–283, 2014.