Comparison of Freeze Software in Anti Forensic using National Institute of Standard and Technology Method

Carto Ardiyanto
Department of Informatics
Universitas Ahmad Dahlan
Yogyakarta of Indonesia

Imam Riadi
Department of Information System
Universitas Ahmad Dahlan
Yogyakarta of Indonesia

ABSTRACT

The development of technology brings rapid changes in the fields of software, hardware and brain ware. Solid State Drive (SSD) is generally used as an operating system container because it is considered more efficient. To reduce maintenance costs for frequently used software such as Deep Freeze, Shadow Defender and Reboot Restore Rx. But software like this can also be exploited for computer crimes, such as removing original data so that an investigator can't find the evidence, he's looking for a trial. it is commonly called Anti-forensic. Previous research on one of the software freezes turned out to be able to inhibit investigators from working. However, there is no definite comparison for each software freeze. To reveal these facts, research was made that is able to display the results of the analysis of the scenarios that have been designed using digital forensic science.The objects of this research are three virtual OS that have been manipulated in the form of steganography in freeze mode Deep Freeze, Shadow Defender and Reboot Restore RX. Methods in collecting data are literature study, experimental and simulation techniques. The stages of the research carried out were starting from looking for literature references, designing case simulations, analyzing simulation and research needs, running case simulations. Next, look for digital evidence to find the third difference in the success or effectiveness of software freezing to become anti-forensic using the National Institute of Standards and Technology method with stages in the form of collection, examination, analysis, and reporting. The results obtained were, in the search for digital evidence, the examination process did not go well. The success rate of software freeze in inhibiting the examination process on a virtual operating system is very high. The operating system installed with the Deep Freeze application has an effectiveness of 93.23%, the Shadow Defender application is 90%, and the Reboot Restore RX application is 100%. Shows software freezes are proven to be effective for investigations on storage forensics cases

Keywords

Digital Forensics, Anti-forensics, software freeze, NIST

1. INTRODUCTION

Technological developments continue to drive change, including in the areas of software, hardware, and human behavior[1]. One of them is computer storage devices as digital document [2].

Currently, computer storage devices are divided into two types, namely volatile and non-volatile[3]. Solid State Drive (SSD) is a piece of hardware that functions as a computer storage media tool that belongs to non-volatile memory[4].SSD users are getting higher every time as in Figure 1.

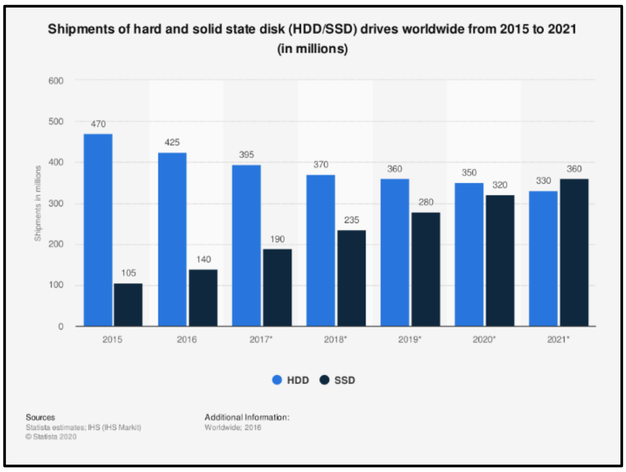


Figure1:SSD Usage Statistics 2015 until 2021

Figure 1 explain,SSD usage has dominated when compared to its predecessor Hard Disk Drives (HDD) around the world, data from statistica.com in years of 2015 until 2021[5].

A good computer storage media is a storage medium that is often maintained physically or non-physically.For example,on non-physical by using software freeze. But this software can also be used for computer crimes.Crimes that can occur in the use of freezing software are anti-forensic techniques in the digital forensics process.Anti-forensic is an effort to prevent, destroy, destroy or eliminate evidence that makes it difficult or impossible to examine an investigator[6].

Researchon frozen SSD using shadow defender software proves that the software is able to make files not restored properly during the examination process carried out using a method in digital forensics.Based on the research evidence, it can be concluded that the software freeze is capable of being an anti-forensic[7]. This research is intended to carry out further research on this freezing software on the anti-forensic process by looking for differences in facts from the existing results. Freezing software in question include Reboot Restore RX, Deep Freeze and Shadow Defender[8]. Using the National Institute of Standards and Technology (NIST) method. NIST method is a general method that is most often used in conducting digital forensics on digital evidence with the stages of collection, examination, analysis and reporting.

2. LITERATURE STUDY

2.1. Computer Storage Media

Storage media is a device or media used to store data or programs [9]. Computer storage media is divided into two parts, namely volatile and non-volatile memory (NVM). which is included in NVM is SSD.

2.2. Digital Forensic

Digital forensics is a branch of forensic science in investigating digital evidence for the sake of legal evidence [10]. In addition, according to the journal [11]digital forensics is an important tool for solving computer crimes committed by computers.

2.3. Anti-Forensics

Anti-forensics according tois a series of tactics and actions carried out by someone based on the desire to thwart the digital investigation process[12].There are several basic categories in anti-forensic[13].

2.3.1.Data Hiding

Data hiding is an anti-forensic category where the original data is hidden or inserted into other data, as well as changing the original data structure[14]. One of the techniques is steganography and encryption[15].

2.3.2.Artefact Wiping

Artifact wiping is a tool to clean up artifacts that are already available. Examples that fall into this category are the degaussing technique[16].

2.3.3. Trail Obfuscation

Trail obfuscation is a way to confuse the trail so that evidence cannot be obtained. Spoofing techniques fall into this category as well as anonymous Virtual Private Network (VPN) and Secure Shell (SSH)[17].

2.3.4 Attacks on processes or tools forensic

In this category, anti-forensic activities are carried out on the forensic process against the procedure itself so that the investigation process can be stopped at the same time[18].

2.3. Freeze Software

Software freeze is software designed to freeze the drive so that the drive cannot perform activities such as writing, changing data files, installing software, or infecting the drive with malware[19].

2.4. Effectiveness Formula

To display a set of numerical data into a solid and clear conclusion, it is necessary to change the percentage, and look for the value of success or effectiveness. The percentage formula can be seen in formula 2.1.

means:

$$X\ (\%) = \frac{\text{Suitability}}{\text{Search}} \times 100 \quad (2,1)$$

X = Percentage.
Matches = total matches found from total file searches.
Search = total files searched.

To get total percentage value of the entire search group can be searched by modifying the average formula, the results of the modified formula can be seen in formula 2.2

means:

$$Tp\ (\%) = \frac{\sum\left(XKp\ A(\%) + \cdots + Xkp\ n\ (\%)\right)}{\sum \text{Kp}} (2,2)$$

Tp = Total percentage of the whole
XKp A = Freeze Application search group.
XKp n = Steganography Tool search group.
Kp = Number of Search groups.

Then, value of effectiveness of software freeze into anti-forensic can be calculated using the formula 2.3.

means:

$$K(\%) = 100\% - Tp\ (\%)(2,3)$$

K = Software Freeze Success
Tp = Total Percentage Overall.

3. METHODOLOGY

3.1. Crime Case Simulation

This case scenario is in the form of an explanation of the stages in the crime committed against the evidence. The purpose of this scenario is to shorten the investigation in obtaining digital evidence which will then be continued by observing and analyzing the results of the observations that occur. The planned case scenario is shown in Figure 2.

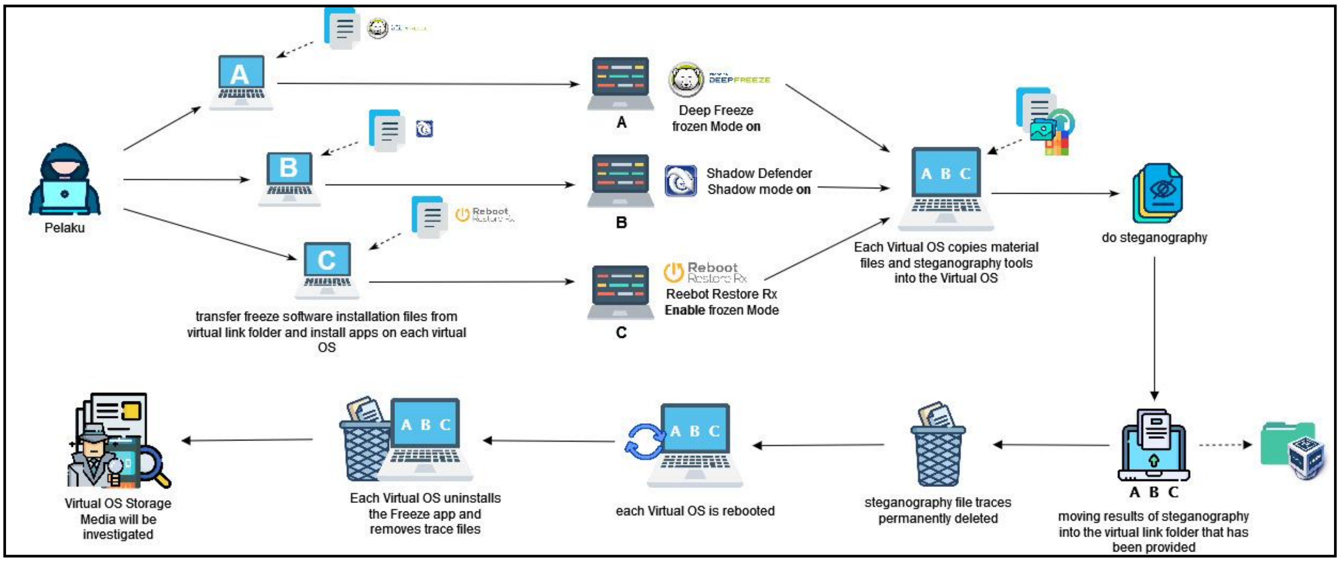

A
A
DEEPFREEZE
Deep Freeze frozen Mode on
Pelaku
B
B
Shadow Defender Shadow mode on
C
C
Reboot Restore Rx
Reebot Restore Rx Enable frozen Mode
transfer freeze software installation files from virtual link folder and install apps on each virtual OS
A B C
Each Virtual OS copies material files and steganography tools into the Virtual OS
do steganography
A B C
moving results of steganography into the virtual link folder that has been provided
steganography file traces permanently deleted
A B C
each Virtual OS is rebooted
A B C
Each Virtual OS uninstalls the Freeze app and removes trace files
Virtual OS Storage Media will be investigated

Figure2:Crime Simulation

Based on Figure 2, perpetrators doing same activities in different Virtual Operating Systems (VOS) with different software in VirtualBox, then perform the action of modifying files, namely steganography with freeze mode that is lit on VOS with the end of the scenario that the virtual data storage media is completely clean after use. After doing this research scenario, it will be continued at the stage of investigating evidence in the form of VOS storage media.

3.2. Research Stages

The stages of research will be carried out in this study have been arranged in Figure 3.

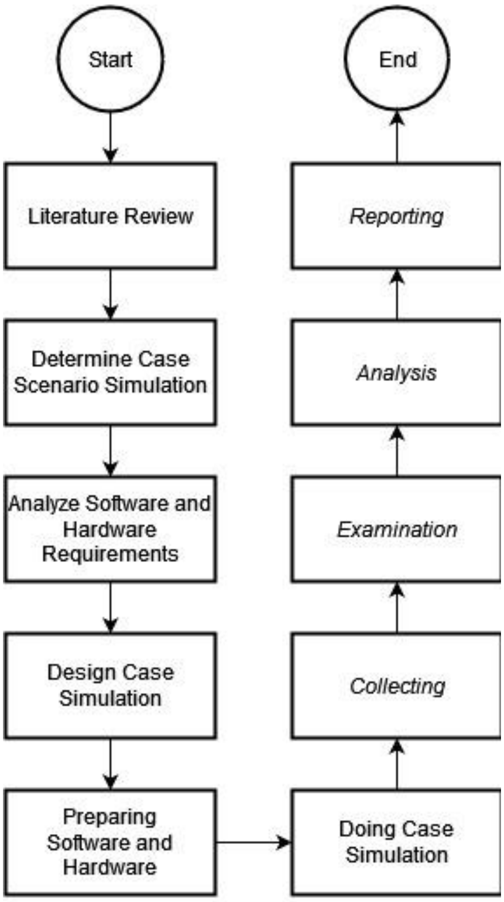

Start
Literature Review
Determine Case Scenario Simulation
Analyze Software and Hardware Requirements
Design Case Simulation
Preparing Software and Hardware
Doing Case Simulation
Collecting
Examination
Analysis
Reporting
End

Figure3:Flowchart Research Stages

Figure 3 describes the research starting from using literature studies to find references then determining simulation case scenarios[20].Then analyzing device requirements, and starting to design simulations, then conducting simulations using the National Institute of Standards and Technology methods to get conclusions,

3.3.1.National Institute of Standard and Technology Method

NIST method has four stages, namely Collection, Examination, Analysis, Reporting. the flow of stages is in Figure 4.

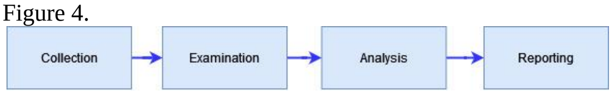


Figure 4:Flow of Process Forensic National Institute of Standard and Technology Method

Figure 4 is a NIST stage flow, this method has been proven to be suitable for storage cases. forensics begins after the case simulation is run.

1) *Collection*, Process starts with namely identifying, labeling, and collecting data. then acquire the operating system virtual storage media using FTK Imager and check the hash code of the acquisition using HashMyFiles, if it turns out that the hash code is different than it will be re-acquired, if the same then the file will be saved.
2) *Examination*, this stage extracts the image files suspected of being a crime using an autopsy application in order to search for files that can be used as evidence in court on the results of the virtual OS acquisition. Where after this stage will proceed to the analysis stage.
3) *Analysis*, after the file has been extracted using autopsy, the next step is to search for files and analyze the artifacts. The flow starts from identifying the data to be searched, searching and analyzing data on artifacts that have been found or not found, then save the results of the analysis.
4) *Reporting*, after being assessed as sufficient, the next step is to make a report that has been obtained from the previous analysis. The contents of the report are the results of the analysis of the tools used and the results of the analysis of information data obtained from the digital forensic process itself. And displays the conclusion data based on the formulas 2.1, 2.2, and 2.3.

4. RESULT AND DISCUSSION

4.1. Collection

The collection stage begins after the simulation is done, the first step is to collect the existing evidence. the evidence found can be seen in Table 1.

Table 1. Physical Evidence Found during Collection.

No	Evidence	Picture	Description
1	Laptop perpetrators		Asus brand laptop was dead when it was found.
2	Charger Laptop perpetrators		Asus brand charger.

Based on Table 1, a laptop and an Asus brand charger were found belonging to the perpetrator. Then the storage media in VirtualBox was acquired with an FTK imager to prevent damage

to physical evidence found and loss of track[21] .Results are in Table 2.

Table 2. Acquisition Results with FTK Imager from Physical Evidence

Description	File Name	OS	Size	MD5
File Imaging 1	A-DF	Windows 7 32bit	10240 MB	902c4118e406cd62e57fc317244973d5
File Imaging 2	B-SD	Windows 7 32bit	10240 MB	ce99481d908f5a0be3295ad56c2b08b0
File Imaging 3	C-RR	Windows 7 64bit	15360 MB	30d83279c9f7a87378ec665fee7386a9

Table 2 contains information on the acquisition results from FTK Imager, then the acquisition results are checked using HashMyFiles. The results of the checks are listed in Table 3.

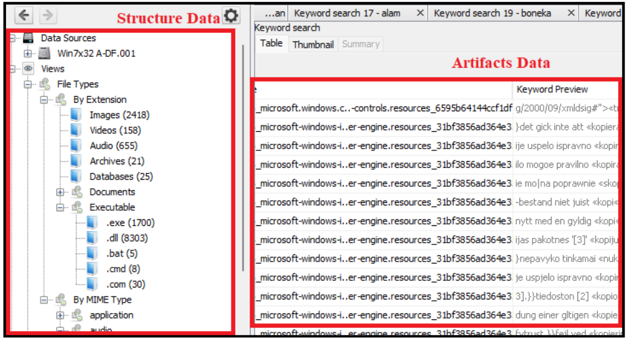
Table 3. Hash Code Value Checked

File Name	MD5	
	Acquisition	HashMyFiles
Win7x32 A-DF	902c4118e406cd62e57fc317244973d5	902c4118e406cd62e57fc317244973d5
Win7x32 B-SD	ce99481d908f5a0be3295ad56c2b08b0	ce99481d908f5a0be3295ad56c2b08b0
Win7x64 C-RR	30d83279c9f7a87378ec665fee7386a9	30d83279c9f7a87378ec665fee7386a9

Table 3, is hash value generated after the acquisition process is complete on each virtual OS using FTK Imager and the results of checking using the HashMyFiles software.The post-acquisition hash value appears to be the same as the hash value in the acquisition file which was checked using HashMyFiles, which means the hash code is valid and worth continuing at the next stage.

4.2. Examination

The examination stage is the extraction stage, all files resulting from the acquisition of each virtual OS file are extracted to search for artifact data to become evidence. extraction is done using autopsy, appearance of file artifacts is in Figure 5.



e	Keyword Preview
_microsoft.windows.c..-controls.resources_6595b64144ccf1df	g/2000/09/xmldsig#">«t
_microsoft-windows-i..er-engine.resources_31bf3856ad364e3	}det gick inte att «kopiera
_microsoft-windows-i..er-engine.resources_31bf3856ad364e3	ije uspelo ispravno «kopir
_microsoft-windows-i..er-engine.resources_31bf3856ad364e3	ilo mogoe pravilno «kopira
_microsoft-windows-i..er-engine.resources_31bf3856ad364e3	ie mo|na poprawnie «sko
_microsoft-windows-i..er-engine.resources_31bf3856ad364e3	-bestand niet juist «kopi«
_microsoft-windows-i..er-engine.resources_31bf3856ad364e3	nytt med en gyldig «kopi«
_microsoft-windows-i..er-engine.resources_31bf3856ad364e3	ijas pakotnes '[3]' «kopiju
_microsoft-windows-i..er-engine.resources_31bf3856ad364e3	}nepavyko tinkamai «nuk
_microsoft-windows-i..er-engine.resources_31bf3856ad364e3	je uspjelo ispravno «kopir
_microsoft-windows-i..er-engine.resources_31bf3856ad364e3	3].}}tiedoston [2] «kopio
_microsoft-windows-i..er-engine.resources_31bf3856ad364e3	dung einer gltigen «kopie
_microsoft-windows-i..er-engine.resources_31bf3856ad364e3	fytrust }}feil ved «kopieri

Figure5:Autopsy Screenshot During Extraction

Based on Figure 5, total data found at the time of extraction are listed in Table 4.

Table 4.Total Extraction Found

Nama	Total File Deleted
Win7x32 A-DF	30310 item
Win7x32 B-SD	8366 item
Win7x64 C-RR	9981 item

In Table 4, there are total items that were deleted in the autopsy, the items found in the form of files with or without extension.

4.3. Analysis

At this stage, the artifact files that have been examined are analyzed using autopsy to obtain digital evidence. The search is focused on engineering crimes, especially on the steganographic techniques carried out. This stage starts from limiting and focusing the search by identifying files that were processed and used in previous crime scenarios. After being identified, all the files are detailed and the identification results are listed in the summary list listed in Table 5.

Table 5.Search File List Summary

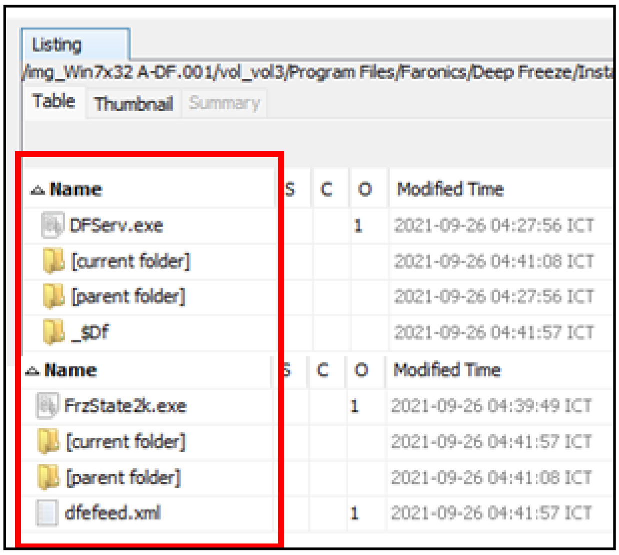
Sub File Name	Total Files Search			File type
	A-BD	B-DF	C-RR	
Freeze Software	41	43	122	file installation, and program
Steganography Tool	31	31	31	file installation, and program
Steganography Materials	10	10	10	.mp3, .jpg, .rar
Steganography Results	8	8	8	.jpg

Based on Table 5, the Software freeze contains installation files, and programs in the form of Deep Freeze, Shadow Defender and Reboot Restore RX. As for steganography is divided into three parts, namely tools, materials and results. From the three sections of steganography, all of them are applied to all image files, two sections have the same list of items, namely tools and materials, while the results section of steganography has a different list of items. All details of the steganography section can be seen in Table 6.

Table 6.SteganographySearchDetail Files

Steganography				
Tools	Materials	Results		
A-BD, B-DF, C-RR	A-BD, B-DF, C-RR	A-BD	B-DF	C-RR
WinRAR 6.10 (folder)	bahan.mp3	alam1.jpg,	alam2.jpg,	alam3.jpg
Silent Installation EN.cmd	bahan.rar	boneka1.jpg	boneka2.jpg	boneka3.jpg
Unpacking portable EN.cmd	alam.jpg,	buku1.jpg,	buku2.jpg,	buku3.jpg,
WinRAR.6.10.exe	boneka.jpg,	kamera1.jpg	kamera2.jpg	kamera3.jpg
WinRarRes(folder)	buku.jpg,	kopi1.jpg	kopi2.jpg	kopi3.jpg
rarreg.key	kamera.jpg,	kucing1.jpg	kucing2.jpg	kucing3.jpg
Settings.reg	kopi.jpg	manusia1.jpg	manusia2.jpg	manusia3.jpg
7zxa.dll	kucing.jpg	parfum1.jpg	parfum2.jpg	parfum3.jpg
Default.SFX	manusia.jpg,			
Default64.SFX	parfum.jpg,			
Descript.ion				
License.txt				
Order.htm				
Rar.exe				
Rar.txt				
RarExt.dll				
RarExt32.dll				
RarFiles.lst				
ReadMe.txt				
UnRAR.exe				
Uninstall.exe				
Uninstall.lst				
WhatsNew.txt				
WinCon.SFX				
WinCon64.SFX				
WinRAR.chm				
WinRAR.exe				
Zip.SFX				
Zip64.SFX				
rarnew.dat				
zipnew.dat				

Based on Table 5 and Table 6, after the search data is summarized, the next step is to conduct a search. All artifact data in each artifact file is combed and searched to find evidence. Then several files were found, the findings obtained from the file search were mostly inconsistent data, such as MFT files, .xml files, etc. But there are also appropriate or similar. Similar findings were separated and recovered immediately for further analysis. As in the findings of A-DF, several files from the freeze application were found, these files are files that are in the program files, A-DF which is shown in Figure 6.



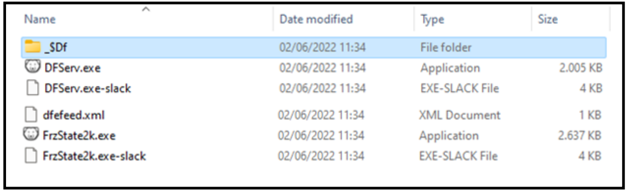
Listing
/img_Win7x32 A-DF.001/vol_vol3/Program Files/Faronics/Deep Freeze/Insta

Name	S	C	O	Modified Time
DFServ.exe			1	2021-09-26 04:27:56 ICT
[current folder]				2021-09-26 04:41:08 ICT
[parent folder]				2021-09-26 04:27:56 ICT
_$Df				2021-09-26 04:41:57 ICT

Name	S	C	O	Modified Time
FrzState2k.exe			1	2021-09-26 04:39:49 ICT
[current folder]				2021-09-26 04:41:57 ICT
[parent folder]				2021-09-26 04:41:08 ICT
dfefeed.xml			1	2021-09-26 04:41:57 ICT

Figure 6:Suspectedly Similar Files in A-DF

Figure 6 shows a file that is suspected to have the same name and extension as the file being sought, namely the Deep Freeze application file [22].Then the suspected file is recovered and then analyzed in terms of metadata and content, after recovering the file as shown in Figure 7.



Name	Date modified	Type	Size
_$Df	02/06/2022 11:34	File folder	
DFServ.exe	02/06/2022 11:34	Application	2.005 KB
DFServ.exe-slack	02/06/2022 11:34	EXE-SLACK File	4 KB
dfefeed.xml	02/06/2022 11:34	XML Document	1 KB
FrzState2k.exe	02/06/2022 11:34	Application	2.637 KB
FrzState2k.exe-slack	02/06/2022 11:34	EXE-SLACK File	4 KB

Figure7:A-DF Similar File Recovered Results

Figure 7, shows the same results as the search file being searched for. There are a total of 8 files that have similarities, including Faronics, Deep Freeze, DFServ.exe, FrzState2k.exe, Install C-0, _$Df, dfefeed.xml, and f0914392.jpg. One of the findings from A-DF is in the form of a .jpg file which has similarities with the sought-after steganographic material file but the name and MD5 value are different from the supposed search file, the difference can be seen in Table 7.

Table 7.Findings on A-DF Differ MD5

File Contents	File Name	Size	Type	MD5
	File Carved			
	f0914392 . jpg	2.69 MB	.jpg	a1c5ccaa68596b2d8e6 3d26060ed9caa
	Steganography Materials			
	kopi.jpg	2.69 MB	.jpg	8166bcf77df997d6137 62192208fe5ae
	Steganography Results			
	kopi1.jpg	7,89 MB	.jpg	517f3484ae993e274d8 79278ad48690a

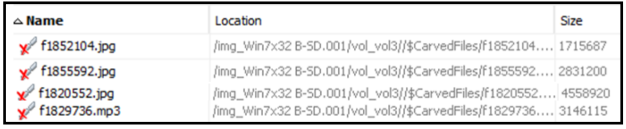
InTable 7, the file extension, size, content is the same, but the file name, with a different MD5 value, this difference is obtained because the file is a file that is already in free space in the operating system memory, so the autopsy replaces the object name with the current name. this was found. then the MD5 value in the file changes[23]. Details of other findings can be seen in Table 8.

Table 8.Result A-DF Found Details

File Name	A-DF (Deep Freeze)
Search File Object	Deep Freeze, WinRAR, Steganography Materials, Steganography Result
Found	- Found 76 files from Deep Freeze search list, 8 same files including Faronics, Deep Freeze, DFServ.exe, FrzState2k.exe, Install C-0, _$Df, dfefeed.xml. - Found 69 files from WinRAR search list / steganography tools but 0 similarities. - Found 18 files from search list for steganography, 1 file is the same, namely f0914392.jpg. - Found 15 files from search list of steganography results but 0 similarities. - Found files with or without extension.

In Table 8, eight A-DF virtual OS files are found that have the same name or extension. This can be used as clue information and temporary digital evidence to measure the effect of Deep Freeze on the extraction work, but due to the different MD5 values, it cannot be validated against the original which was permanently deleted in previous simulations[24].

Then on B-SD (Shadow Defender) after a search, found files that have similar values, the files are in the form of images and audio, with file types .jpg and .mp3. The findings are in Figure 8.



Name	Location	Size
f1852104.jpg	/img_Win7x32 B-SD.001/vol_vol3//$CarvedFiles/f1852104....	1715687
f1855592.jpg	/img_Win7x32 B-SD.001/vol_vol3//$CarvedFiles/f1855592....	2831200
f1820552.jpg	/img_Win7x32 B-SD.001/vol_vol3//$CarvedFiles/f1820552....	4558920
f1829736.mp3	/img_Win7x32 B-SD.001/vol_vol3//$CarvedFiles/f1829736....	3146115

Figure8:B-SD Similar FilesFound Result

In Figure 8 found 4 files that are suspected to have similarities with the object of the file being searched for. The similarities include the contents of the files with the same size, but after further analysis, the names and MD5 values in the files are not the same. Comparison of equations can be seen in Table 9.

Table 9.ComparisonSimilar Found Filesfrom B-SD

No	File Name	Size (MB)	Type	MD5
1	File Carved			
	f0914392. jpg	2.69	.jpg	a1c5ccaa68596b2d8e63d260 60ed9caa
	Steganography Materials			
	kopi.jpg	2.69	.jpg	8166bcf77df997d613762192 208fe5ae
2	File Carved			
	f1852104.j pg	1.63	.jpg	083053e21ae2721298f770af9 e80b4b6
	Steganography Materials			
	kamera.jpg	1.63	.jpg	dfd057854d2093a4971c0dad 363ad822
3	File Carved			
	f1855592.j pg	2.69	.jpg	a1c5ccaa68596b2d8e63d260 60ed9caa
	Steganography Materials			
	kopi.jpg	2.69	.jpg	8166bcf77df997d613762192 208fe5ae
4	File Carved			
	f1829736.	3.00	.mp3	e1d895542d6aa250f82bbe23

	mp3			4291a1a3
	Steganography Materials			
	bahan.mp3	5.38	.mp3	34879a3b09e7944fc048e3b30f90f016

From Table 9, the four files found have similarities with steganographic material files from the form of file contents, file sizes, their extension types, and in metada have in common. But the MD5 value are not the same, the case is same as in the previous A-DF, the file is a file that is already in free space in the operating system memoryand affect the value of MD5. In addition, details of other findings on B-SD can be seen in Table 10.

Table 10.Result B-SDFound Details

File Name	B-SD (Shadow Defender)
Search File Object	Shadow Defender, WinRAR, Steganography Materials, Steganography Result
Found	- Retrieved 77 files from Shadow Defender search list, with 0 similarities. - Found 57 files from the WinRAR search list / steganography tools but 0 similarities. - Found 39 files from the search list for steganographic materials, 4 of which are similar, namely f1820552.jpg, f1852104.jpg, f1855592.jpg, f1829736.mp3. - Found 23 files from the search list of steganography results but 0 similarities. - Found files with extension and no extension.

Table 10 explains, All searches on the B-SD acquisition results found the items sought, but of all the items found, only four files were identified as having the same extension, file content, and size with the object file search list.
Then, on C-RR (Reboot Restore RX), after searching for files, no similar files were found based on the object file search list, along with data in Table 10.

Table 11.Result C-RRFound Details

File Name	C-RR (Reboot Restore RX)
Search File Object	Reboot Restore RX, WinRAR, Steganography Materials, Steganography Result
Found	- Found 51 files from the search list Reboot Restore RX - Found 41 files from WinRAR search list - Found 47 files from the search list for steganography material - Found 25 files from the search list of steganography results. - All files found have nothing in common.

In Table 11, the search did not find the file being searched for from the previously specified target file object, the files found were files that had different extensions, names, sizes and file contents which were not the same file.

4.3. Reporting

Based on the analysis [25], three image files have been used to find evidence of steganographic and anti-forensic crimes. From the results of the analysis using the help of an autopsy application, there are differences in the findings of digital evidence produced. The percentage of these findings can be calculated using formulas 2.1 and 2.2, so the data can be seen in Table 12.

Table 12.Digital Evidence Percentage Difference Found

Nama File Imaging	Sub File Name	Total Searches and Results			Percentage
		Search	Results	Similarity	
A-DF (Deep Freeze)	Freeze Software	41	76	7	17,07%
	SteganographyTools	31	69	0	0%
	Steganography Material	10	18	1	10,00%
	Steganography Result	8	15	0	0%
	Total				6,77%
B-SD (Shadow Defender)	Freeze Software	43	77	0	0%
	Steganography Tools	31	57	0	0%
	Steganography Material	10	39	4	40,00%
	Steganography Result	8	23	0	0%
	Total				10%
C-RR (Reboot Restore RX)	Freeze Software	122	51	0	0%
	Steganography Tools	31	41	0	0%
	Steganography Material	10	47	0	0%
	Steganography Result	8	25	0	0%
	Total				0%

Based on Table 12, the percentages to get the find result are A-DF is 6.77%, B-SD is10%, and C-RR is 0%. From these data, the success of software freeze in the examination process can be calculated using formula 2.3 and could be presented in Table 13.

Table 13.Anti-Forensic Success Percentage

File Freeze Software	Percentage Effectiveness
DeepFreeze	93,23 %
ShadowDefender	90 %
Reboot Restore RX	100 %

From Table 13,calculation of the success of the software freeze shows that Deep Freeze is able to inhibit the extraction process with a value of 93.23%, in the Shadow Defender software the success rate of inhibiting the extraction process is 90%, and Reboot Restore RX obtained the largest process in inhibiting the extraction process is 100 %.

5. CONCLUSION

Based on Forensic Analysis with the method of the National Institute of Standard and Technology, it was found that the deleted files, some of which had similarities. On the operating system installed with the Deep Freeze application, the success rate of affecting the inspection process is 93.23%, while on the operating system installed the Shadow Defender application is 90%, and the Reboot Restore RX application has a 100% success rate. The three acquisitions have scores above 90%, this shows that the software freeze is effective as an anti-forensic. On future research it is suggested to collect MD5 data on the search file object before it is permanently deleted for the need for validation of the find file and use a different freeze application, especially the last updated one, not the most popular one. Also use other forensic methods that help speed up the analysis.

6. REFERENCES

[1] I. Riadi, R. Umar, and I. M. Nasrulloh, "Experimental Investigation of Frozen Solid State Drive on Digital Evidence with Static Forensic Methods," *Lontar Komput. J. Ilm. Teknol. Inf.*, vol. 9, no. 3, p. 169, 2018, doi: 10.24843/lkjiti.2018.v09.i03.p06.

[2] I. Riadi and I. M. N. Rusydi Umar, "Forensic Analysis of Digital Evidence on Frozen Solid State Drives Using the National Institute of Standards and Technology (NIST) Method," *J. Insa. Comtech*, vol. 2, no. 2, pp. 33–40, 2017.

[3] T. Firman, "Comparing Storage Device Performance: SSD vs HDD," *tirto.id*, 2017. https://tirto.id/membandingkan-kinerja-perangkatpenyimpan-data-ssd-vs-hdd-crSk (accessed Apr. 24, 2021).

[4] M. Riskiyadi, "Forensic Investigation of Digital Evidence in Exposing Cybercrime," *CyberSecurity dan Forensik Digit.*, vol. 3, no. 2, pp. 12–21, 2020.

[5] T. Alsop, "Shipments of hard and solid state disk (HDD/SSD) drives worldwide from 2015 to 2021," *Statista.com*,2021.https://www.statista.com/statistics/285474/hdds-and-ssds-in-pcs-global-shipments-2012-2017/ (accessed Apr. 24, 2021).

[6] G. C. Kessler, "Anti-forensics and the digital investigator," *Proc. 5th Aust. Digit. Forensics Conf.*, pp. 1–7, 2007, doi: 10.4225/75/57ad39ee7ff25.

[7] I. Riadi and I. M. Nasrulloh, "Forensic Analysis of Solid State Drives (SSD) Using the Grr Rapid Response Framework Forensic Analysis of Solid State Drives (SSD) Using The Grr Rapid Response Framework," *J. Teknol. Inf. dan Ilmu Komput.*, vol. 6, no. 5, pp. 509–518, 2019, doi: 10.25126/jtiik.201961516.

[8] N. Klein, "Backblaze Drive Stats for Q1 2021," *Backblaze*,2021.https://www.backblaze.com/blog/backblaze-hard-drive-stats-q1-2021/ (accessed Jul. 09, 2021).

[9] D. T. Yuwono, A. Fadlil, and S. Sunardi, "Performance Comparison of Forensic Software for Carving Files using NIST Method," *J. Teknol. dan Sist. Komput.*, vol. 7, no. 3, pp. 89–92, 2019, doi: 10.14710/jtsiskom.7.3.2019.89-92.

[10] W. Pranoto, I. Riadi, and Y. Prayudi, "Comparison of Forensics Tools on NVMe SSD TRIM Features Using Live Forensics Method," *It J. Res. Dev.*, vol. 4, no. 2, pp. 135–148, 2020, doi: 10.25299/itjrd.2020.vol4(2).4615.

[11] S. L. Garfinkel, "Digital forensics research: The next 10 years," *Digit. Investig.*, vol. 7, no. SUPPL., pp. S64–S73, 2010, doi: 10.1016/j.diin.2010.05.009.

[12] B. Rahardjo and I. P. A. E. Pratama, "Anti-Computer Forensic Testing And Analysis Using Shred Tool," *Lontar Komput. J. Ilm. Teknol. Inf.*, vol. 7, no. 2, p. 104, 2016, doi: 10.24843/lkjiti.2016.v07.i02.p04.

[13] N. A. Sultan, K. H. Thanoon, and O. A. Ibrahim, "Ethical Hacking Implementation for Lime Worm Ransomware Detection," *J. Phys. Conf. Ser.*, vol. 1530, no. 1, 2020, doi: 10.1088/1742-6596/1530/1/012078.

[14] S. Lasaharu and I. Riadi, "Network Forensic on Web-based Applications using Network Forensic Development Life Cycle Method," *Int. J. Comput. Appl.*, vol. 183, no. 47, pp. 8–14, 2022, doi: 10.5120/ijca2022921869.

[15] Z. Rahma and I. Riadi, "Email Forensic from Phishing Attack using Network Forensics Development Life Cycle Method," *Int. J. Comput. Appl.*, vol. 183, no. 46, pp. 36–42, 2022, doi: 10.5120/ijca2022921865.

[16] M. Masri, H. Alam, M. Masri, Z. Lubis, and M. Izhni Pohan, "Byte Error Correction Simulation Using Hamming Code," *Journal of Electrical Technology*, vol. 4, no. 3. pp. 2502–3624, 2019.

[17] T. Rochmadi, "Live Forensics for Anti-Forensic Analysis on a Web Browser Case Study Browzar," *Indonesian Journal of Business Intelligence (IJUBI)*, vol. 1, no. 1. p. 32, 2019, doi: 10.21927/ijubi.v1i1.878.

[18] A. I. Putra, R. Umar, and A. Fadlil, "Forensic Analysis Video Metadata Authenticity Detection Using Exiftool," *Semin. Nas. Inform. 2018 (semnasIF 2018)*, vol. 2018, no. November, pp. 21–25, 2018.

[19] F. Corporation, "DFS_GettingStarted.pdf." 2022, [Online].Available:https://www.faronics.com/assets/DFS_GettingStarted.pdf.

[20] D. L. Tri Yusnanto, "Optimizing the Use of CMD and Sysinternalsuits as Malware Detection," *Jurnal Transformasi*, vol. 15, no. 1. pp. 66–74, 2019.

[21] A. Hadi and S. Riadi, Imam, "Digital Evidence Forensics on NVMe Solid State Drives (SSDs) Using National Institute of Standards and Technology (NIST) Methods," *Semnastek 2019*, pp. 551–558, 2019.

[22] winrar, "Winrar 6.11," *win.rar GmbH*. https://www.win-rar.com/start.html?&L=0.

[23] F. Carbone, *Computer Forensics with FTK*. 2014.

[24] M. Wazid, A. Katal, R. H. Goudar, and S. Rao, "Hacktivism trends, digital forensic tools and challenges: A survey," *2013 IEEE Conf. Inf. Commun. Technol. ICT 2013*, no. Ict, pp. 138–144, 2013, doi: 10.1109/CICT.2013.6558078.

[25] I. Riadi, R. Umar, and I. M. Nasrulloh, "Digital Forensic Analysis on Frozen Solid State Drive With National Institute of Justice (NIJ) Method," *Elinvo (Electronics, Informatics, Vocat. Educ.*, vol. 3, no. 1, pp. 70–82, 2018, doi: 10.21831/elinvo.v3i1.19308.