JURNAL ECOTIPE
Electronic, Control, Telecommunication, Information, and Power Engineering

Volume 11, Issue 1, April 2024, pp. 88-96
ISSN 2355-5068 ; e-ISSN 2622-4852
DOI: 10.33019/jurnalecotipe.v11i1.4489

Forensic Investigation of Digital Evidence on Flash Disk with Forensic Process Method Based on NIST

Febriand Gysberth Pariela Zamsari[1], Teguh Wahyono[2]
[1,2] Program Studi Teknik Informatika, Universitas Kristen Satya Wacana, Salatiga, 50715, Indonesia

ARTICLE INFO

Article history :

Received : 07/03/2024
Revised : 24/03/2024
Accepted : 15/04/2024

Keywords:

Autopsy; Digital Forensics; Flash disk; FTK Imager

ABSTRACT

Flash disk is a tool that is inseparable from daily life. With flash disks, users can keep important data for personal or company. Apart from that, in lots of cases Indonesian law uses flash disks as evidence. ITE Law (Law Information and Transactions Electronics) regulates how the provision of digital evidence becomes strong evidence in court. This research investigates forensics to digital evidence on a flash disk with four scenario tests. Processing digital forensics uses a forensic process based on guide National Institute of Standards and Technology (NIST). This research produces an analysis where the evidence processed with scenarios 1 and 4 are valid digital evidence to be submitted to the court, while evidence 2 and 3 are invalid evidence.

Corresponding Author:

Febriand Gysberth Pariela Zamsari
Informatics Engineering, Universitas Kristen Satya Wacana, Salatiga, 50715, Indonesia
Email: febriandgysberth67@gmail.com

1. INTRODUCTION

In the current era, the use of storage media like disk free or flash disks. It's not what's new and inseparable in daily life. Flash disk are often used for keeping some perceived data important to its users, for example, personal data or important information for an individual or company. However, it cannot be denied that sometimes there is an individual or group that has the intention to be active in illegal activity like data theft, distribution of malware, and so on [1].

Cybercrime develops from time to time along with the development of technology, no one can deny that sometimes digital evidence is often contained in storage media like flash disks. This issue has been proven and written down in several cases in Indonesia, via the Directory website Judgment in 2023, which can be searched with the keyword "flash disk *digital forensik*". There were 6,701 cases and in between were 138 ITE (Information and Transactions Electronics) crime cases related to flash disks [2].

Decision results prove that in case-related crimes with ITE in Indonesia, the perpetrator crime keeps evidence on a flash disk memory. A temporary law regarding ITE that applies in Indonesia is contained in law Number 19 of 2016 concerning Information and Transactions Electronics [3]. Based on the Constitution, information electronic or document electronic is legally valid evidence in a way law in Indonesia. Document electronics stores information in a way electronics that can be accessed through computer or system electronics, which includes text, sound, images, and similar shapes, which convey possible meanings understood by capable individuals.

In addition to this article, it is contained in article 6 which explains that information electronic or document electronic is considered legitimate in a way applicable in Indonesia if digital evidence can be accessed, displayed, guaranteed its integrity, and can be accountable which explains some circumstances [4]. Therefore, that's important to understand and prove the method of storage, modification, and deployment of digital evidence so you can be accountable in the eyes of the law, especially for related parties with the law. This matter is necessary for moreover deeply related validity of digital evidence, such as cases where digital evidence was initially stored in the flash disk that has been deleted can be considered valid.

National Institute of Standards and Technology (NIST) published guidelines to help analyze digital forensics for digital evidence on published storage media with code publication NIST SP 800-86. There are four stages important from NIST publication SP 800-86 in do or carry out digital forensics stages : Collection, Examination, Analysis, and Reporting [5]. With hope after four stages, they can prove that they found existing digital evidence deleted on a flash disk that can be given information structured for describing, explaining, use and place forensic information is valid evidence at court [6].

There are several studies related to digital forensics, the journal article entitled "Forensic Investigation of Remnant Data on USB Storage Devices Sold in New Zealand" focuses on the investigation forensics of residual data on the device storage flash disk. The author evaluates three tools imaging forensics sources open, namely DC3DD, DCFLDD, and Guymager, based on established criteria by the National Institute of Standards and Technology (NIST) [7]. They make case testing, analyzing functionality, and usage of hard device and consume time from every tool and compare it’s performance. This research found that most parts of flash disk purchased in New Zealand contains sensitive personal and organizational data. A journal article entitled “Static Forensics on USB Mass Storage Use Forensics Toolkit Imager” discusses the use of digital forensics on USB mass storage was experimented to obtain digital evidence of USB mass storage. Furthermore, the evidence will be processed using the Static Forensics and Forensics Toolkit Imager. Discussion results shows that the method of Static Forensics can be used in a way that is safe and valid to take digital evidence of USB mass storage [8]. Forensics Toolkit Imager is also proven to help in the extraction and processing process of digital evidence with more effectiveness and efficiency [9].

See importance validity a digital evidence, this research will do willing case investigation forensics in flash disk, to see is digital evidence in flash disk valid or not. Investigation forensics done with the use of method Forensic Process based on NIST standards. This research also involves utilization and comparison results from various analysis tools, namely the use of Autopsy and Access Data FTK imager. Application from methods that will be researched can give strong clarify and accurate results to digital evidence. The research was conducted to investigate that digital evidence based on the findings of the investigation can be a valid tool or evidence and support the trial process. For example, in the investigation there are things that support digital evidence that can incriminate the results of the verdict in the eyes of the law.

2. RESEARCH METHODS

The writer will apply a method that has been published by the National Institute of Standards and Technology (NIST) in publication NIST SP 800-86. The research’s flow can be seen in Figure 1 below.

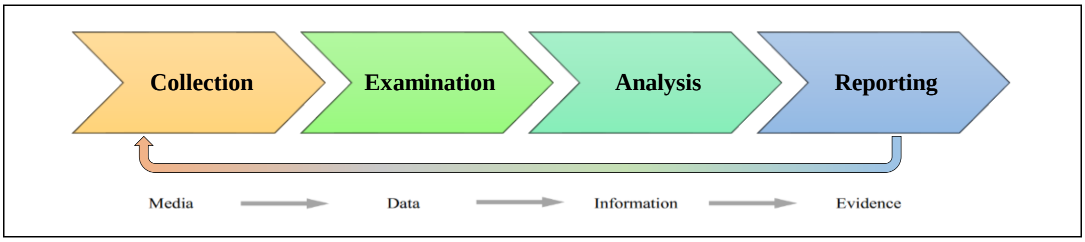


Figure 1. Forensic process

Based on Figure 1, there are 4 stages in the Forensic Process, namely Collection, Examination, Analysis, and Reporting. Following is an explanation of these stages.

2.1. Collection Stage (Data Collection)

This stage is the process of collecting related data with incidents or things you are looking for that will be identified, labeled, recorded, and collected, with guard integrity of the data [14]. So, it can be used as anevidence from flash disk and also stuff existing digital evidence inside. At this stage, the writer will create a scenario where someone provides a flash disk as evidence to be submitted to the court and

Volume 11, Issue 1, April 2024, pp. 88-96
ISSN 2355-5068 ; e-ISSN 2622-4852
DOI: 10.33019/jurnalecotipe.v11i1.4489

the writer examines whether the flash disk is valid evidence or not in court, by creating four supporting examination scenario schemes.

First, flash disk saves 10 files considered original as digital evidence and there is no changes or deletions against 10 files. Second, the flash disk contains 10 original files however, there are 8 files on it. Third, the flash disk contains 10 original files and differences were found between files and the original file. Fourth, the flash disk with 10 original files, there is a modification name from files.

2.2. Examination Stage (Data Processing)

This stage explains tools and techniques appropriate for forensics with the type of data collected will be used for identifying and extracting information relevant from the data that has been collected and guarding the integrity of the data [15]. The tools and materials used in this research as follows:

Table 1. Tools used in research

Name Tools	Specification	Information
A laptop	ASUS TUF Gaming F15, i7-10870H 2.20GHz, 8GB, Windows 11 home single language, x64-based PC	Hardware and operating system
USB flash disk	SanDisk USB *Flash disk*, 16GB	Hardware test
Autopsy	Autopsy 4.20.0 (RELEASE)	Forensic software
AccessData FTK imager	AccessData ® FTK® Imager 4.7.1.2	Forensic software
HashCalc	Version 2.02	Hash validity software

2.3. Analysis Stage (Data Analysis)

This stages involves analysis from results inspection to get information and useful conclusions in answering questions or targets that become motivation for data collection and examination [16]. This stage is supported by analyzing the results investigation from FTK Imager and Autopsy applications, after that produced conclusion that answer the questions or targets where the conclusion is valid or not.

2.4. Reporting Stage

The final stage involves delivery results analysis, which covers explanations about actions that have been taken, determined action necessary additions done, as well as recommendation to repair the policies, guidelines, procedures, tools, and other aspects of the forensic process [17].

3. RESULTS AND DISCUSSION

3.1. Collection Stage

In the collection stage, evidence is collected in the flash disk which currently equipped with 10 pieces of digital evidence with file extensions such as, *.docx, .pdf, .mp3, .MOV, .jpg, .zip, .xlsx, .ppt, .exe and .txt* where each file own mark hashes the original will make as reference during this research.

Table 2. Reference values results hash from files original on the flash disk

File Name	MD5 Value
Document format	
[BBD]1.txt	72788458fbe6bf211a54ff730d2c1233
[BBD]2.pdf	a0323007b43cde8d6a097f06999458f1
[BBD]3.doc	25fedabace3c2022c8dacf3761f95d60
[BBD]4.pptx	ca71ae171d962d3e54880c595be9bb1e
[BBD]5.xlsx	bef9e6d9db570eafb928d7b379b49edb
Image Formats	
[BBD]6.jpg	1fe95ec5e459a88813447a4f01f89550
Audio Formats	
[BBD]7.mp3	fe01262c6e4be7e3100bb38a91853f47
Video Format	
[BBD]8.MOV	939f968f2dc99df6e69d828e7074bca6
Compression Format	
[BBD]9.zip	78cc17258dcfeacb4b306e39ad93204a
Executable Format	
[BBD]10.exe	0161434334901af384ab9453d61a13d2

3.2. Examination Stage

In this stage where the flash disk evidence is inserted into the USB port of the digital forensic evidence execution laptop, by activate the USB Write Protector followed by matching the hash value with the help of the HashCalc application and FTK imager. FTK imager is used to create data clones or data imaging as digital evidence from flash disks. Next, the results of FTK imager data imaging are matched with the results of the hash value using HashCalc and FTK imager so that the results obtained are as follows:

Table 3. Matching results imaging data with flash disk

Scheme	MD5 Flash Disk	MD5 Imaging	Status Verification
SCHEME 1	3d8a64b73ac85c6a722cd263452bf7d6	3d8a64b73ac85c6a722cd263452bf7d6	VALID
SCHEME 2	b72e142c73a46bf9f4986972bf16cc28	b72e142c73a46bf9f4986972bf16cc28	VALID
SCHEME 3	0ec8d660ad9e982c3f54793c863fe531	0ec8d660ad9e982c3f54793c863fe531	VALID
SCHEME 4	2dfc42fc0ec1dd0cbd6656659bfb25da	2dfc42fc0ec1dd0cbd6656659bfb25da	VALID

3.3. Analysis Stage

Based on results obtained after doing imaging data, such digital evidence is analyzed more and becomes digital evidence using FTK Imager and Autopsy to obtain more results maximum.

A. Scheme 1: flash disk saves 10 files considered original as a digital evidence and no change or deletion against 10 files. In scheme 1, FTK Imager and Autopsy software were successful in getting 10 files digital evidence with the hash value, after matched with the hash value reference in table 4.1 is obtained the result as follows :

Table 4. Validation results Scheme 1 uses FTK Imager and Autopsy

File Name	MD5	Original	Results Status
Document format			
[BBD]1.txt	72788458fbe6bf211a54ff730d2c1233	72788458fbe6bf211a54ff730d2c1233	VALID
[BBD]2.pdf	a0323007b43cde8d6a097f06999458f1	a0323007b43cde8d6a097f06999458f1	VALID
[BBD]3.doc	25fedabace3c2022c8dacf3761f95d60	25fedabace3c2022c8dacf3761f95d60	VALID
[BBD]4.pptx	ca71ae171d962d3e54880c595be9bb1e	ca71ae171d962d3e54880c595be9bb1e	VALID
[BBD]5.xlsx	bef9e6d9db570eafb928d7b379b49edb	bef9e6d9db570eafb928d7b379b49edb	VALID
Image formats			
[BBD]6.jpg	1fe95ec5e459a88813447a4f01f89550	1fe95ec5e459a88813447a4f01f89550	VALID
Audio formats			
[BBD]7.mp3	fe01262c6e4be7e3100bb38a91853f47	fe01262c6e4be7e3100bb38a91853f47	VALID
Video format			
[BBD]8.MOV	939f968f2dc99df6e69d828e7074bca6	939f968f2dc99df6e69d828e7074bca6	VALID
Compression format			
[BBD]9.zip	78cc17258dcfeacb4b306e39ad93204a	78cc17258dcfeacb4b306e39ad93204a	VALID
Executable format			
[BBD]10.exe	0161434334901af384ab9453d61a13d2	0161434334901af384ab9453d61a13d2	VALID

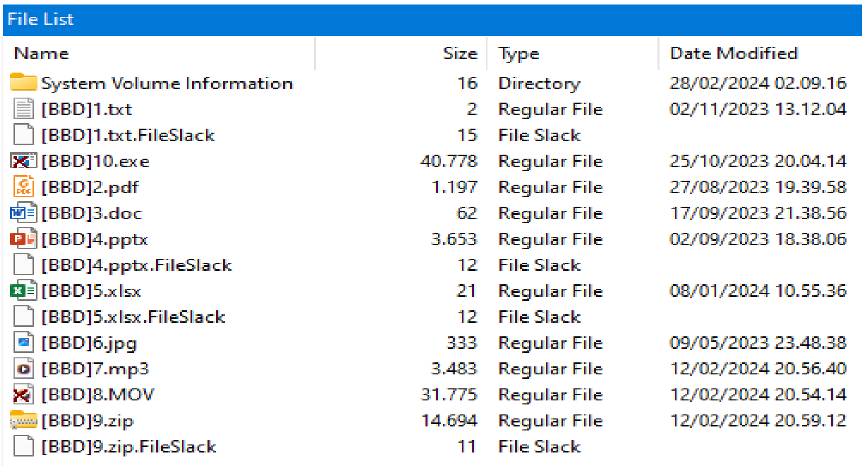
Table 4 produce 10 imaging files from the original flash disk and there is no difference value with the result hash both FTK Imager and Autopsy software, so digital evidence in scheme 1 is considered valid and can be submitted as valid digital evidence.

B. Scheme 2: the flash disk contains 10 original files, but there are only 8 files on the flash disk. In scheme 2, FTK Imager and Autopsy software were manage to get 8 original files of evidence and there were 2 original files of evidence. The evidence was erased on the flash disk along with its hash value. After being matched with the hash value reference in Table 4.1, the results were as follows:

Table 5. Validation results Scheme 2 uses FTK Imager and Autopsy

File Name	MD5	Original	Results Status
Document format			
[BBD]1.txt	72788458fbe6bf211a54ff730d2c1233	72788458fbe6bf211a54ff730d2c1233	VALID
[BBD]2.pdf	a0323007b43cde8d6a097f06999458f1	a0323007b43cde8d6a097f06999458f1	VALID
[BBD]3.doc	25fedabace3c2022c8dacf3761f95d60	25fedabace3c2022c8dacf3761f95d60	VALID
[BBD]4.pptx	ca71ae171d962d3e54880c595be9bb1e	ca71ae171d962d3e54880c595be9bb1e	VALID
[BBD]5.xlsx	bef9e6d9db570eafb928d7b379b49edb	bef9e6d9db570eafb928d7b379b49edb	VALID
Image formats			
[BBD]6.jpg	1fe95ec5e459a88813447a4f01f89550	1fe95ec5e459a88813447a4f01f89550	VALID
Audio formats			
[BBD]7.mp3	fe01262c6e4be7e3100bb38a91853f47	fe01262c6e4be7e3100bb38a91853f47	VALID
Video format			
[BBD]8.MOV	939f968f2dc99df6e69d828e7074bca6	939f968f2dc99df6e69d828e7074bca6	VALID
Compression format			
[BBD]9.zip	78cc17258dcfeacb4b306e39ad93204a	78cc17258dcfeacb4b306e39ad93204a	VALID
Executable format			
[BBD]10.exe	0161434334901af384ab9453d61a13d2	0161434334901af384ab9453d61a13d2	VALID

The results from Table 5 still same to produce 10 files equipped with a hash value of 10 files. However, both software also detects deletion of evidence files.

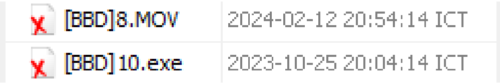


File List

Name	Size	Type	Date Modified
System Volume Information	16	Directory	28/02/2024 02.09.16
[BBD]1.txt	2	Regular File	02/11/2023 13.12.04
[BBD]1.txt.FileSlack	15	File Slack	
[BBD]10.exe	40.778	Regular File	25/10/2023 20.04.14
[BBD]2.pdf	1.197	Regular File	27/08/2023 19.39.58
[BBD]3.doc	62	Regular File	17/09/2023 21.38.56
[BBD]4.pptx	3.653	Regular File	02/09/2023 18.38.06
[BBD]4.pptx.FileSlack	12	File Slack	
[BBD]5.xlsx	21	Regular File	08/01/2024 10.55.36
[BBD]5.xlsx.FileSlack	12	File Slack	
[BBD]6.jpg	333	Regular File	09/05/2023 23.48.38
[BBD]7.mp3	3.483	Regular File	12/02/2024 20.56.40
[BBD]8.MOV	31.775	Regular File	12/02/2024 20.54.14
[BBD]9.zip	14.694	Regular File	12/02/2024 20.59.12
[BBD]9.zip.FileSlack	11	File Slack	

Figure 2. Results of imaging scheme 2 FTK Imager

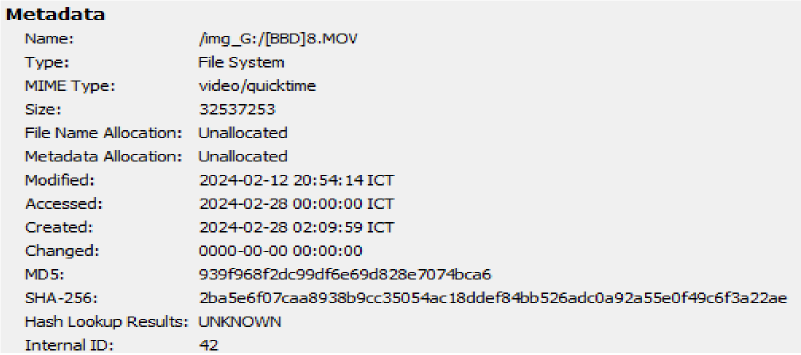
The output results from Scheme 2 use FTK Imager to detect and find there are two items of deleted digital evidence with Name files [BBD]8.MOV and [BBD]10.exe. This deletion is evidenced by the icon image of existing files cross-red.



[BBD]8.MOV	2024-02-12 20:54:14 ICT
[BBD]10.exe	2023-10-25 20:04:14 ICT

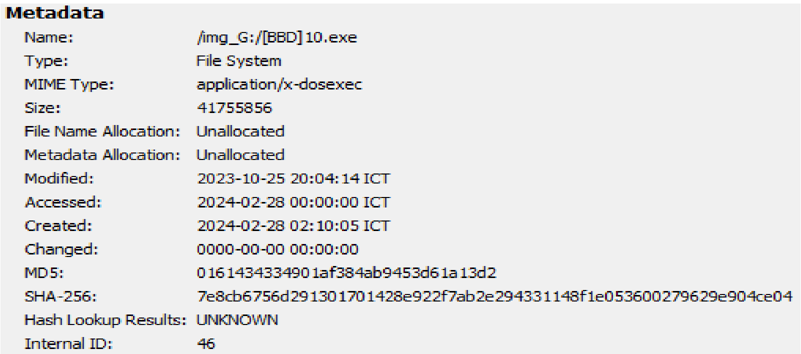
Figure 3. Imaging results of Autopsy Scheme 2

The output results from Scheme 2 use Autopsy also detect and find there are two items of deleted digital evidence with Name files [BBD]8.MOV and [BBD]10.exe and verified with the file icon containing sign cross-red.



```
Metadata
  Name:                    /img_G:/[BBD]8.MOV
  Type:                    File System
  MIME Type:               video/quicktime
  Size:                    32537253
  File Name Allocation:    Unallocated
  Metadata Allocation:     Unallocated
  Modified:                2024-02-12 20:54:14 ICT
  Accessed:                2024-02-28 00:00:00 ICT
  Created:                 2024-02-28 02:09:59 ICT
  Changed:                 0000-00-00 00:00:00
  MD5:                     939f968f2dc99df6e69d828e7074bca6
  SHA-256:                 2ba5e6f07caa8938b9cc35054ac18ddef84bb526adc0a92a55e0f49c6f3a22ae
  Hash Lookup Results:     UNKNOWN
  Internal ID:             42
```

Figure 4. Item metadata digital proof [BBD]8.MOV



```
Metadata
  Name:                    /img_G:/[BBD]10.exe
  Type:                    File System
  MIME Type:               application/x-dosexec
  Size:                    41755856
  File Name Allocation:    Unallocated
  Metadata Allocation:     Unallocated
  Modified:                2023-10-25 20:04:14 ICT
  Accessed:                2024-02-28 00:00:00 ICT
  Created:                 2024-02-28 02:10:05 ICT
  Changed:                 0000-00-00 00:00:00
  MD5:                     0161434334901af384ab9453d61a13d2
  SHA-256:                 7e8cb6756d291301701428e922f7ab2e294331148f1e053600279629e904ce04
  Hash Lookup Results:     UNKNOWN
  Internal ID:             46
```

Figure 5. Item metadata digital proof [BBD]10.exe

This deletion is evidence with metadata from second files where allocation name files produce unallocated (no allocated) and file metadata allocation produces unallocated. Validation results scheme 2 in table 6 and table 7 as well as evidence deletion on the flash disk, in image 4 and image 5 can be concluded that evidence with scheme 2 is invalid because there are two files already deleted, files with names [BBD]8.MOV and [BBD]10.exe.

C. Scheme 3: Where the flash disk hash value 10 files original and found difference content from files with the original files. In scenario 3, both FTK Imager and Autopsy software were successful in getting 10 files digital evidence with hash value, after matched with the hash value reference in table 4.1 is obtained the result as follows :

Table 6. Validation results Scheme 3 uses FTK Imager and Autopsy

File Name	MD5	Original	Results Status
Document format			
[BBD]1.txt	72788458fbe6bf211a54ff730d2c1233	72788458fbe6bf211a54ff730d2c1233	VALID
[BBD]2.pdf	a0323007b43cde8d6a097f06999458f1	a0323007b43cde8d6a097f06999458f1	VALID
[BBD]3.doc	e6acb86d922ddef7f52f925ebafc8870	25fedabace3c2022c8dacf3761f95d60	**INVALID**
[BBD]4.pptx	d9a2465f75f61330d77d3e48576aea79	ca71ae171d962d3e54880c595be9bb1e	**INVALID**
[BBD]5.xlsx	bef9e6d9db570eafb928d7b379b49edB	bef9e6d9db570eafb928d7b379b49edb	VALID
Image formats			
[BBD]6.jpg	1fe95ec5e459a88813447a4f01f89550	1fe95ec5e459a88813447a4f01f89550	VALID
Audio formats			
[BBD]7.mp3	fe01262c6e4be7e3100bb38a91853f47	fe01262c6e4be7e3100bb38a91853f47	VALID
Video format			
[BBD]8.MOV	939f968f2dc99df6e69d828e7074bca6	939f968f2dc99df6e69d828e7074bca6	VALID
Compression format			
[BBD]9.zip	78cc17258dcfeacb4b306e39ad93204a	78cc17258dcfeacb4b306e39ad93204a	VALID
Executable format			
[BBD]10.exe	0161434334901af384ab9453d61a13d	0161434334901af384ab9453d61a13d2	VALID

.

Analysis results from Scheme 3 are proven with Table 6, both software can analyze and find 10 files on the flash disk but there is a change value on digital evidence with Name files [BBD]3.doc and [BBD]4.pptx.

Table 7. Artifact data from digital evidence [BBD]3.doc

Type	Value	Source
Date Modified	2024-02-28 03:54:00 ICT	org.sleuthkit.autopsy.keywordsearch.KeywordSearch IngestModule
Program Name	Microsoft Office Word	org.sleuthkit.autopsy.keywordsearch.KeywordSearch IngestModule
Last Printed Date	2021-07-03 07:35:00 ICT	org.sleuthkit.autopsy.keywordsearch.KeywordSearch IngestModule
Date Created	2023-09-15 16:37:00 ICT	org.sleuthkit.autopsy.keywordsearch.KeywordSearch IngestModule
User ID	-A- 3373 2020	org.sleuthkit.autopsy.keywordsearch.KeywordSearch IngestModule
Owner	Adhi	org.sleuthkit.autopsy.keywordsearch.KeywordSearch IngestModule
Source File Path	/img_G:/[BBD]3.doc	
Artifact ID	-9223372036854775806	

Table 7 is output from results scheme 3, where Autopsy software displays when digital evidence file [BBD]3.doc created and when the last time the file was changed and by whom. From the table can be known that file [BBD]3.doc was first created by Adhi on September 15 2023 at 16:37:00 ICT (Indochina Time) and carried out modification fill file by -A- 3373 2020 on February 28, 2024 at 03:54:00 ICT (Indochina Time).

Table 8. Artifact data from digital evidence [BBD]4.pptx

Type	Value	Source
Date Modified	2024-02-28 03:51:19 ICT	org.sleuthkit.autopsy.keywordsearch.KeywordSearch IngestModule
Program Name	Microsoft Office PowerPoint	org.sleuthkit.autopsy.keywordsearch.KeywordSearch IngestModule
Date Created	2006-08-16 00:00:00 ICT	org.sleuthkit.autopsy.keywordsearch.KeywordSearch IngestModule
User ID	-A- 3373 2020	org.sleuthkit.autopsy.keywordsearch.KeywordSearch IngestModule
Source File Path	/img_G:/[BBD]4.pptx	
Artifact ID	-9223372036854775800	

Table 8 is output from results scheme 3, where Autopsy software displays when digital evidence file [BBD]4.pptx created and when the last time the file was changed and by whom. From the table can be known that the [BBD]4.pptx file was first created on August 16, 2006 at 00:00:00 ICT (Indochina Time) and carried out modification content file by -A- 3373 2020 on February 28, 2024 at 03:51:19 ICT (Indochina Time).

The results of scheme 3, as evidenced by table 6 supplemented by table 7 and table 8, prove that there are changes in the contents of the files of digital evidence [BBD]3.doc and [BBD]4.pptx, it can be concluded that the digital evidence is invalid and cannot be used as digital evidence to support the court.

D. Scheme 4 : flash disk saves 10 considered original files as digital evidence and there is modification name or date on the digital file. In scheme 4, both FTK Imager and Autopsy software were successful in getting 10 files digital evidence with the mark the hash, after matched with hash value reference in table 4.1 is obtained the result as follows :

Table 9. Validation results Scheme 4 uses FTK Imager and Autopsy

File Name	MD5	Original	Results Status
Document format			
[BBD]1.txt	72788458fbe6bf211a54ff730d2c1233	72788458fbe6bf211a54ff730d2c1233	VALID
[BBD]2.pdf	a0323007b43cde8d6a097f06999458f1	a0323007b43cde8d6a097f06999458f1	VALID
[BBD]3.doc	25fedabace3c2022c8dacf3761f95d60	25fedabace3c2022c8dacf3761f95d60	VALID
[BBD]4.pptx	ca71ae171d962d3e54880c595be9bb1e	ca71ae171d962d3e54880c595be9bb1e	VALID
[BBD]5.xlsx	bef9e6d9db570eafb928d7b379b49edb	bef9e6d9db570eafb928d7b379b49edb	VALID
Image formats			
[BBD]6.jpg	1fe95ec5e459a88813447a4f01f89550	1fe95ec5e459a88813447a4f01f89550	VALID
Audio formats			
[BBD]7.mp3	fe01262c6e4be7e3100bb38a91853f47	fe01262c6e4be7e3100bb38a91853f47	VALID
Video format			
[BBD]8.MOV	939f968f2dc99df6e69d828e7074bca6	939f968f2dc99df6e69d828e7074bca6	VALID
Compression format			
[BBD]9.zip	78cc17258dcfeacb4b306e39ad93204a	78cc17258dcfeacb4b306e39ad93204a	VALID
Executable format			
[BBD]10.exe	0161434334901af384ab9453d61a13d2	0161434334901af384ab9453d61a13d2	VALID

The final result obtained after operating scheme 4, both FTK Imager and Autopsy software can find and analyze 10 files of digital evidence. There is no difference hash value of the 10 files tested, this signifies that scheme 4 with no change with hash value even though the file name is changed but it still can be qualified to be submitted as digital evidence.

3.4. Reporting Stage

Based on the results of the result analysis stage, it can be concluded that the digital evidence contained in the flash disk and executed according to Scheme 1 and Scheme 4 are valid. It can be seen from the display of the two processes in the software that there is no replacement or change in the hash value results. Thus, there is no defect in the authenticity of the evidence and can support material evidence to the judge in accordance with the provisions contained in ITE Law Number 19 of 2016. Meanwhile, digital evidence with scheme 2 cannot be used as digital evidence because there are deletions from the original file. Therefore, the flash disk does not qualify as digital evidence and is submitted to the court, scheme 3 also cannot be used as valid evidence due to changes in the contents of the original files [BBD] 3.doc and [BBD] 4.pptx.

The results stage report is also supported by expert lecturer, Dr. Jeferson Kameo, S.H., LLM at the Faculty of Law, Satya Wacana Christian University. He supports and agrees that the results of schemes 1 and 4 can be considered as valid evidence, because there is no change in the hash value which states that the deleted digital evidence has not been edited and qualifies as evidence according to the Electronic Information and Transaction Law (UU ITE) in Indonesia. Meanwhile, digital evidence schemes 2 and 3, cannot fulfill the elements to be submitted as digital evidence. The results of scheme validation and evidence analysis show the deletion of files and changes in the hash value of files that affect the authenticity of a file.

4. CONCLUSION

Thus, based on the test results in scheme 1 and scheme 4, it is valid evidence because there is no change in the hash value, which states that digital evidence that has been erased has not undergone editing and meets the requirements as evidence according to the ITE Law Number 19 of 2016. Meanwhile, the results of scheme 2 and 3 where digital evidence is deleted or edited from flash disk are considered invalid and do not qualify to be submitted as digital evidence. FTK Imager and Autopsy applications are capable of executing, producing, as well as finishing what to expect from the writer by the scheme that has been made. FTK Imager can analyze in a relative short time, Autopsy can do more analysis complex and deeper. With the use these two tools, the writer can finish a scheme with faster and also obtainable maximum results. Future researcher is expected to implement different scenarios and schemes as well as supported by the latest hardware and software can produce updates in different cases.

Volume 11, Issue 1, April 2024, pp. 88-96
ISSN 2355-5068 ; e-ISSN 2622-4852
DOI: 10.33019/jurnalecotipe.v11i1.4489

REFERENCE

[1] Barkem W, Sidabutar J. Digital Forensic Analysis of WhatsApp Business Applications on Android-Based Smartphones Using NIST. MATRIX J Management, Inform Tech and Comput Engineering 2023;22:615–26. https://doi.org/10.30812/matrik.v22i3.3033.

[2] Clerk of the Court. Directory of Decisions nd https://bangunan3.mahkamahagung.go.id/.

[3] RI UN 19 T 2016. Law of the Republic of Indonesia Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Information and Electronic Transactions. Law No. 19 of 2016 2016:1–31.

[4] Sunarmi, Mahmud Mulyadi IMDKMA. Juridical Analysis of Digital Evidence in Proving Hate Speech Crime Cases in Medan District Court Decision No. 3168/Pid.Sus/2018/Pn.Mdn. Res Nullius Law J 2021;3:98–117. https://doi.org/10.34010/rnlj.v3i2.3862.

[5] Kent K, Chevalier S, Grance T, Dang H. Guide to Integrating Forensic Techniques into Incident Response. Natl Inst Stand Technol 2006.

[6] Vishnu Budi, Aan Widayat Kusban, Muhammad SM. Computer Forensic Analysis to Support the Investigation Process in Crime Cases 2015:12.

[7] Shah Z, Kyaw A, Truong HP, Ullah I, Levula A. Forensic Investigation of Remnant Data on USB Storage Devices Sold in New Zealand. Appl Sci 2022;12. https://doi.org/10.3390/app12125928.

[8] Mahardika Sulaksono P, Santoso B. Static Forensics on USB Mass Storage Using Forensics Toolkit Imager. J Comput Ther 2022;8:132–42. https://doi.org/10.35143/jkt.v8i1.5334.

[9] Muhammad Nur Al-Azhar. Series 1 Digital Forensics: General Guide to Digital Forensics on Windows, Linux, Mac & Mobile Platforms. Salemba Infotek Publisher; 2021.

[10] Hassan NA. Digital Forensics Basics. Digit Forensics Basics 2019. https://doi.org/10.1007/978-1-4842-3838-7.

[11] Hassan NA. Introduction: Understanding Digital Forensics. Digit Forensics Basics 2019:1–33. https://doi.org/10.1007/978-1-4842-3838-7_1.

[12] Mega Rosita. Comparative Analysis of the Performance of FTK IMAGER and AUTOPSY in Digital Forensics on *Flash disks* . Crypto Info 2023;17. https://doi.org/10.56706/ik.v17i3.83.

[13] Jr MP, Arnaldy D, TP S, Si M. Digital Document Integrity Analysis in the Digisign UTD PNJ Application Using Digital Signatures. RepositoryPnjAcId nd

[14] Yuliana D, Yuniati T, Zen BP. Analysis of Digital Evidence of Cyberbullying on Social Media Using the National Institute of Standards and Technology (Nist) 800-101 Method. LEDGER J Inform Inf Technol 2022;1:113–23. https://doi.org/10.20895/ledger.v1i3.812.

[15] Abdillah MF, Prayudi Y. Data Recovery Comparative Analysis using Open-based Forensic Tools Source on Linux. Int J Adv Comput Sci Appl 2022;13:633–9. https://doi.org/10.14569/IJACSA.2022.0130975.

[16] Aditya Gunawan CT, Suryanto Y. Maturity Level Analysis of Digital Evidence Handling on Integrated Criminal Justice System based on NIST SP800-53 Revision 5 Using NIST Maturity. Budapest Int Res Critics Inst 2022:10481–97. https://doi.org/10.33258/birci.v5i2.4861.

[17] Aushaf RF, Ismail SJI, ... Implementation of Digital Forensics in Telegram on the Operating System. eProceedings … 2021;7:2767–78.