Scientific Journal of Informatics
Vol. 10, No. 4, Nov 2023

p-ISSN 2407-7658 http://journal.unnes.ac.id/nju/index.php/sji e-ISSN 2460-0040

Forensic Tools Comparison on File Carving using Digital Forensics Research Workshop Framework

La Jupriadi Fakhri[1*], Imam Riadi[2], Anton Yudhana[3]
[1]Master Program of Informatics, Universitas Ahmad Dahlan, Yogyakarta, Indonesia
[2]Department of Information System, Universitas Ahmad Dahlan, Yogyakarta, Indonesia
[3]Department of Electrical Engineering, Universitas Ahmad Dahlan, Yogyakarta, Indonesia

Abstract.
Purpose: Cybercrime is the misuse of technology as a tool or medium in committing crimes such as hacking, stealing, deleting, hiding, and destroying information. Cybercriminals tend to delete, hide, and format all the data collected to eliminate traces of digital evidence. In digital forensics, file carving techniques can overcome data loss from storage media. This study aims to determine the results of the file carving process in uncovering digital evidence and evaluating the performance of digital forensic software, including Foremost and Scalpel, based on 3 assessment parameters.
Methods: In this investigation, the Digital Forensics Research Workshop (DFRWS) research method is used with the following stages: Identification, Preservation, Collection, Examination, Analysis, and Presentation.
Results: Comparison results of the data obtained from Foremost and Scalpel forensic tools are based on three primary parameters including the speed of the recovery process, the number of successfully recovered files, and the identical hash value. The Foremost tool managed to recover the carving files in 1 minute and 3 seconds, showing a success rate of 85% with a hash value similarity rate of 70.59%. On the other hand, Scalpel recovered the carving file in 2 minutes 17 seconds, achieving a success rate of 65% with a hash value similarity rate of 7.69%.
Novelty: This data results from the performance of both forensic tool applications in collecting digital evidence from Flash disk storage media.

Keywords: File carving, Foremost, Scalpel, Flash disk, DFRWS
Received August 2023 / **Revised** November 2023 / **Accepted** November 2023

INTRODUCTION

The industrial world is increasing rapidly and the development of information technology today is so fast and makes it easy for humans to overcome the problems they face [1]–[3]. Along with the advancement of information technology, the use of computers and digital devices has become pervasive in almost all aspects of human life. However, there is a dark side behind this progress, including cybercrime activities [4], [5]. Cybercrime is misusing technology to commit criminal acts such as hacking, stealing data, spreading malware, and other activities that harm individuals and organizations [6]–[8]. Based on a report published on the website of the Directorate of Cyber Crime of the National Police, from July 2022 to July 2023, there were 1,856 reports related to cybercrime [9]. Cybercrime is becoming increasingly complex and diverse due to the emergence of various techniques and methods to infiltrate, damage, or steal data from computer systems and digital devices [10]–[14]. The technique used by cyber criminals is to disguise digital traces, such as deleting or hiding important data that can become evidence of crime [15]–[18]. A common technique often used is deleting or destroying data [19]–[21] to eliminate evidence that can be used to track and prove their criminal acts.

Data deletion techniques can be done by various methods, including manual deletion, the use of specialized software, and the use of malware to corrupt data [22]–[24]. Law enforcement plays an important role in gathering valid and robust digital evidence to expose and prosecute cyber criminals [25], [26]. This process involves the retrieval of evidence from computer devices or digital storage media that are relevant to criminal cases. However, if the evidence obtained has been deleted or hidden, digital evidence recovery

[*]Corresponding author.
Email addresses: la2007048015@webmail.uad.ac.id (Fakhri), imam.riadi@is.uad.ac.id (Riadi), eyudhana@ee.uad.ac.id (Yudhana)
DOI: 10.15294/sji.v10i4.46901

becomes challenging for law enforcement. This problem can be solved with digital forensic techniques, including file carving. The file carving technique is an important digital forensic technique to identify and retrieve deleted or hidden files from digital storage media [27]–[29]. The tools used in the file carving technique are Foremost and Scalpel. The performance of these tools can be measured based on three main parameters: the speed of file recovery, the number of files successfully recovered, and the percentage of correctness of the recovered files [30]–[33].

Cybercrimes require a basic forensic framework to make the investigation process more structured. There are many frameworks commonly used, including the National Institute of Justice (NIJ) [34], National Institute of Standard and Technology (NIST) [35]–[40], Digital Forensics Research Workshop (DFRWS) [41]–[43], and Association of Chief Police Officers (ACPO) [44]. In this research, the investigation process on digital evidence uses the DFRWS framework. DFRWS was chosen because it has a standardized and consistent forensic framework that can provide ease of use and is easily understood by technical or non-technical users [45].

Research using the DFRWS framework, as described in [46] entitled "Syntactical Carving of PNGs and Automated Generation of Reproducible Datasets" indicates that the application of the syntactical PNG file carver was able to restore 98% of the test files correctly and completely, while the rest 2% of the files were unsuccessfully recovered. Another study used the DFRWS framework for digital forensics on high-capacity Secure Digital. The results indicated that 77% of the files could be recovered at the examination stage using the Foremost tool, and the file recovery accuracy was 50% with the string file hash validation [47]. Similar research also utilizes the DFRWS Framework, described in [48] entitled "Mobile Forensic Analysis of Signal Messenger Application on Android using DFRWS Framework." Digital evidence was found from the Signal Messenger application, including application information, account information, conversations, images, videos, contacts, and stickers. The results of this study show that the Belkasoft Evidence Center forensic tool achieved the highest accuracy rate of 78.69%, Magnet AXIOM achieved 26.23%, and MOBILedit Forensic Express achieved 9.84%.

Another research uses the DFRWS framework to perform Audio Forensics on smartphones. The results of this study show that the Oxygen Forensic application successfully obtained digital evidence in the form of two audio files and two video files on a smartphone. About 90% of the data was identical to the original voice recording, while only 10% of the data was not identical [49]. Another similar study that adopts the DFRWS Framework is "Mobile Forensic Investigation of Fake News Cases on Instagram Applications with DFRWS Framework," as described in [50]. The digital evidence includes accounts, emails, images, videos, URLs, times, IP addresses, and locations. The results of this study show that the Magnet Axiom application succeeded in obtaining digital evidence by 87.5%, while the Cellebrite UFED application reached 68.75%.

Based on the background of the problem, the main focus of this research is to analyze the performance of data recovery software (file carving) with a static forensic approach in revealing digital evidence using the Digital Forensics Research Workshop (DFRWS) Framework. This research aims to evaluate the performance of two digital forensics software, Foremost and Scalpel. The evaluation considers three aspects, namely the speed of the recovery process, the number of files successfully recovered, and the similarity of hash values successfully restored. The test samples consist of two files with two different extension formats, namely images (jpg) and documents (pdf).

METHODS

Research Stages

This research uses the Digital Forensics Research Workshop (DFRWS) framework. The DFRWS stages focus on the identification, preservation, collection, examination, analysis, and presentation. Figure 1 shows the stages of the forensic process [49].

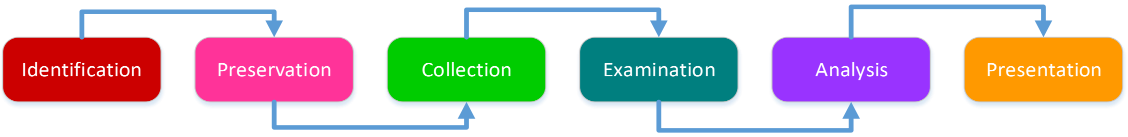


Figure 1. Stages in the DFRWS method

Figure 1 explains the application of the DFRWS method in the process of investigating evidence related to file carving cases on flash disk storage media. The stages of the DFRWS method are as follows [51]:

1) Identification
   At this stage, the investigator conducts an examination to determine the need for the investigation and the type of evidence required.
2) Preservation
   This is a critical process to maintain the integrity and authenticity of the evidence and prevent claims that the evidence has been destroyed.
3) Collection
   At this stage, the investigator collects data that is considered important and can support the further analysis process.
4) Examination
   In the examination stage, the investigator analyzes and scrutinizes previously collected data sources. This process involves filtering certain parts of the data sources to find relevant information, but without changing the data content because the authenticity of the data is essential.
5) Analysis
   The analysis stage is crucial to find out the origin of the data, where it came from, how it was created, and the purpose of the data. At this stage, the investigator delves deeper to understand the information behind the data collected. By understanding the origin and creation of the data, the investigator can make conclusions about the authenticity and relevance of the digital evidence found.
6) Presentation
   The presentation stage is a step to present information about the analysis results in detail, clearly, and informatively.

Tools and Materials

A list of tools used in this study is listed in Table 1.

Table 1. Research tools used

No	Name	Specification	Information
1	Laptop	Acer Nitro 5 core i5	Hardware
2	Operating System	Arc-Linux	OS
3	DC3DD	OpenSource Forensic Application	Software
4	Foremost	OpenSource Forensic Application	Software
5	Scalpel	OpenSource Forensic Application	Software

Table 1 shows the tools used in this research, consisting of one hardware, one operating system, and three software. In addition, the digital evidence used in this research is in the form of documents and images checked for hash values in each file. The results are listed in the following Table 2.

Table 2. Evidence copied on Flash disk

No	Original File Name	File Format	Hash Value (MD5)
1	Data 1	.jpg	d69b3cb77770d0f9fe4ac00fd88c7790
2	Data 2	.jpg	9c1448ecc578e796ea8dd41819a7a584
3	Data 3	.jpg	8e760c6624ede1e0c196a8cecda3a1fb
4	Data 4	.jpg	958c9010cb0c4e61bebda8c3e4110b91
5	Data 5	.jpg	7d1d037d48b2fe72a4dad3117c208582
6	Data 6	.jpg	e9f08b33b25ce3e514c9d7aa899a887d
7	Data 7	.jpg	fa250fbef2d97ba627fb294ba5eb574c
8	Data 8	.jpg	72078bc9733df809664bcfa606f4d95d
9	Data 9	.jpg	6f0801785d8cd74113dc9ab5d0af8155
10	Data 10	.jpg	03ed38261563ca7e14874ced0cfa6daa
11	Data 11	.pdf	30bd2736b7783973863dc1c2db913169
12	Data 12	.pdf	ba406ef9734d5fdd6910ac1ac427bf80
13	Data 13	.pdf	817ed96ea4f4fd24169771acdfb9c0ea
14	Data 14	.pdf	db798d6b6d47e790afbb60058120a6ca
15	Data 15	.pdf	bd452566ded58cbd0e806ed56db053fd
16	Data 16	.pdf	cbd4fcd5db0aa5c0059f1b6409353366
17	Data 17	.pdf	86710fcc8748d46c6fb05c5a15833eb4
18	Data 18	.pdf	8ed974d04204265ffafee9dc8305647f
19	Data 19	.pdf	74abac532beb852d2cda61a444f907df
20	Data 20	.pdf	95bc17cf311ff9fe170a2cc4aacabd32

Table 2 shows 20 examples of digital evidence files used in the file carving method as research material. There are ten .jpg image files and ten .pdf document files . This data reflects common file types often found in storage devices such as computers and smartphones. The sampling was conducted on July 15, 2023. Each file in this sample has been hashed using the MD5 algorithm to verify its integrity during the acquisition and forensic analysis process. This data is an essential part of the research to test the ability of forensic tools to recover and reconstruct deleted or hidden files.

Comparison Method

The comparison uses digital forensic tools based on each available forensic data. Furthermore, the comparisons to determine the results of quantitative numbers need to use the percentage formula in equation (1) [52].

$$Par = \frac{\sum ar0}{\sum arT} \times 100\% \qquad (1)$$

In Equation 1, Par is the accuracy index value of forensic tools, $\sum ar0$ is the number of material parameters obtained, and $\sum ar0$ is the total number of material parameters used.

Case Study

The case study aims to facilitate the identification process when analyzing digital evidence. The evidence secured is storage media in the form of a flash disk in a state of death or not being active on the computer. The object of research as digital evidence used is the result of fictitious data found in a crime involving the theft of company data and stored in flash disk through the file carving method. Figure 2 shows the scenario related to the electronic evidence object in the form of a flash disk.

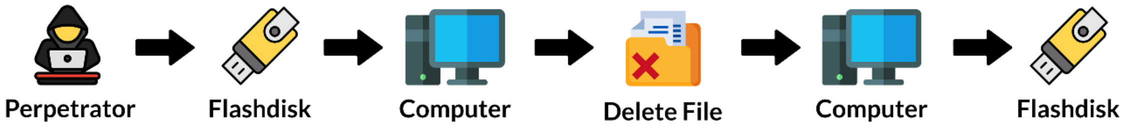


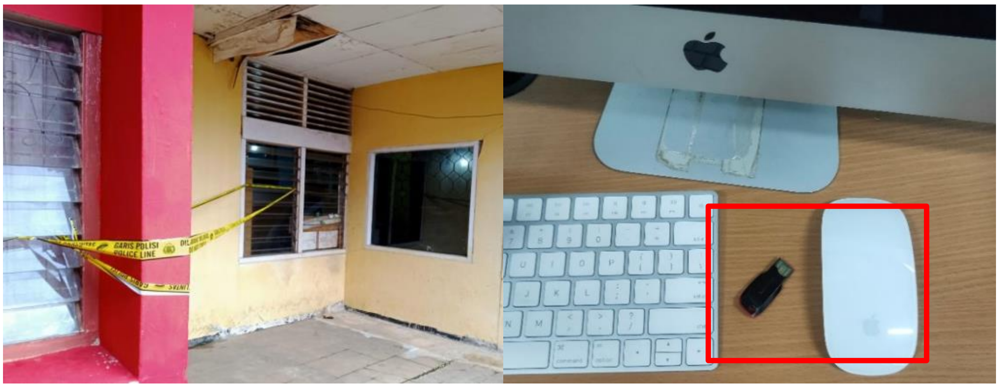
Figure 2. The scenario of deleting evidence on a flash disk

Figure 2 depicts a scenario related to an electronic evidence object in the form of a flash disk. Through the visualization, it appears that the flash disk used to store company data has been thrown away by the perpetrator of the crime to eliminate traces. Later, the flash disk is found by the authorities and taken as evidence. However, when the flash disk was examined, it turned out that the perpetrator had deleted most of its data. As a step to restore the lost data, a file carving process was performed on the flash disk.

RESULTS AND DISCUSSIONS

Identification

The evidence identification process begins with securing the crime scene in the perpetrator's workspace, as shown in Figure 3.



(a) Crime case (b) Evidence

Figure 3. Securing the crime scene and obtaining evidence

Figure 3 (a) shows the prevention of access by unauthorized parties to the place, so the evidence is maintained and not affected by unauthorized parties. After the crime scene security is complete, the next step is to search for evidence by examining the entire crime scene area and identifying anything that could potentially be relevant evidence. This process is done carefully to ensure that no evidence is overlooked. The evidence search results, as seen in Figure 3 (b), show that the police found electronic evidence on the perpetrator's workspace table.

Preservation

The second step is to ensure that the flash disk used as evidence is appropriately preserved. This aims to prevent physical damage to the flash disk and potential data loss during the investigation process. The container or packaging must meet security and protection standards, so there is no manipulation, alteration, or damage to the flash disk during the investigation. The packaging process of the original evidence is shown in Figure 4.

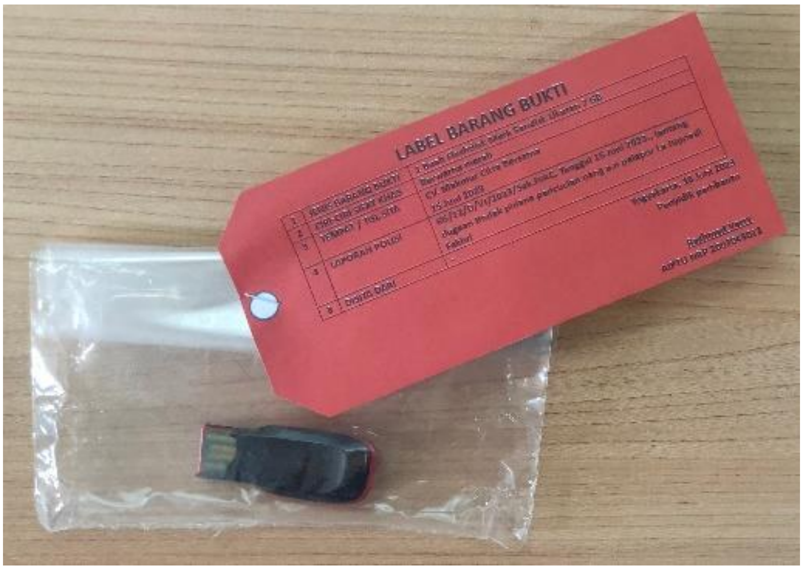


Figure 4. Packaging of original evidence

As shown in Figure 4, packaging the original Flash disk must be carefully executed and well-documented. Strict security measures and proper record-keeping ensure that the Flash disk remains in the same condition as it was found at the crime scene, thus maintaining the integrity of the digital evidence. Important information about Flash disk is presented in the following table.

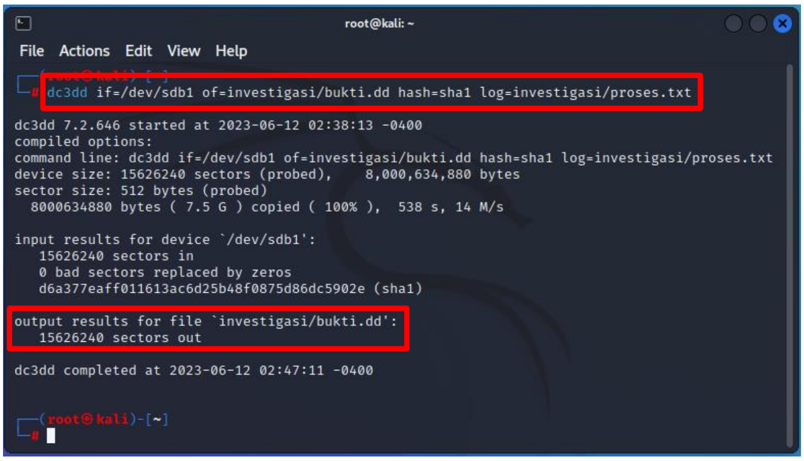
Table 3. Research tools used

Evidence	Brand	Specification	Serial Number
Flash disk	SanDisk Cruzer Blade	Data Traveler G3, 8 GB, FAT32	4C530100870520120075

Table 3 contains important information about the flash disk, including the brand, model, capacity, and serial number. All this information will be carefully and meticulously recorded as an integral part of the documented case record. This information serves as authentic evidence that can support further investigation and analysis. By documenting this information, the authorities will have a strong foundation to maintain the integrity of the evidence and ensure the validity of each step in the related legal process.

Collection

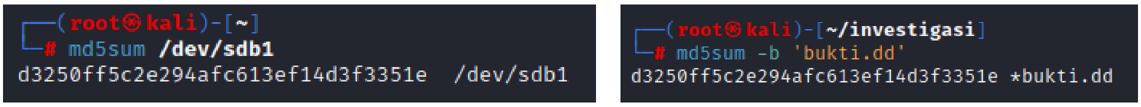
After the flash disk is preserved, the next step is to collect the data from the flash disk. In this case, DC3DD software is used to clone the data on the flash disk. This cloning process aims to make an identical copy of the original flash disk to maintain data integrity, and the original flash disk can still be used as evidence. The data on the flash disk will be copied using the bitstream image method, which allows every bit of the original data, including deleted files, to be reconstructed [53]. The data acquisition process on the physical evidence (Flash disk) is performed using DC3DD software, as shown in the following Figure 5.



```
root@kali: ~
File  Actions  Edit  View  Help
┌──(root㉿kali)-[~]
└─# dc3dd if=/dev/sdb1 of=investigasi/bukti.dd hash=sha1 log=investigasi/proses.txt

dc3dd 7.2.646 started at 2023-06-12 02:38:13 -0400
compiled options:
command line: dc3dd if=/dev/sdb1 of=investigasi/bukti.dd hash=sha1 log=investigasi/proses.txt
device size: 15626240 sectors (probed),    8,000,634,880 bytes
sector size: 512 bytes (probed)
  8000634880 bytes ( 7.5 G ) copied ( 100% ),  538 s, 14 M/s

input results for device `/dev/sdb1':
   15626240 sectors in
   0 bad sectors replaced by zeros
   d6a377eaff011613ac6d25b48f0875d86dc5902e (sha1)

output results for file `investigasi/bukti.dd':
   15626240 sectors out

dc3dd completed at 2023-06-12 02:47:11 -0400


┌──(root㉿kali)-[~]
└─# 
```

Figure 5. Packaging of original evidence

Figure 5 shows that the time required for data acquisition is 9 minutes and 2 seconds. After that, the hash value between the original evidence and the image resulting from the cloning process is verified. This step aims to ensure that the cloned evidence to be examined is identical to the original evidence [45]. Hash value comparison can be seen in Figure 6.



```
┌──(root㉿kali)-[~]
└─# md5sum /dev/sdb1
d3250ff5c2e294afc613ef14d3f3351e  /dev/sdb1
```

(a) Hash value of original evidence

```
┌──(root㉿kali)-[~/investigasi]
└─# md5sum -b 'bukti.dd'
d3250ff5c2e294afc613ef14d3f3351e *bukti.dd
```

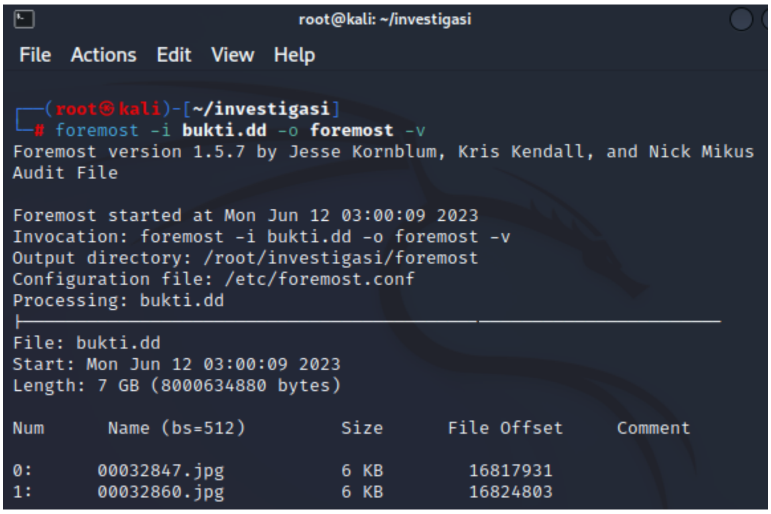
(b) Hash value of cloned evidence

Figure 6. Hash value of evidence and acquisition proceeds

The verification process in Figure 6 (a) and Figure 6 (b) shows an identical hash value of "d3250ff5c2e294afc613ef14d3f3351e." From these results, it can be concluded that the cloned evidence file is completely identical to the original evidence. This ensures the integrity of the data and the authenticity of the digital evidence used in the investigation process. With the hash value match, the investigation can proceed to the examination stage.

Examination

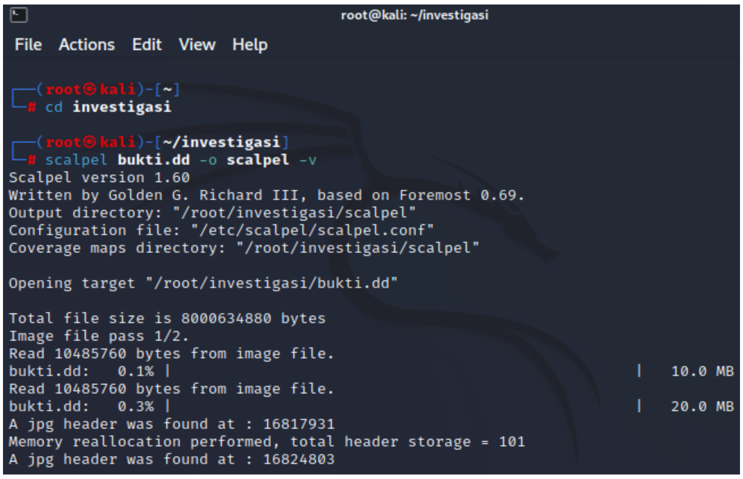
After the data cloning process using DC3DD software is complete, the next step is to examine the data using Foremost and Scalpel software. This process aims to identify and retrieve files that have been deleted or hidden in the cloned file. The process of restoring carved files using Foremost software can be seen in Figure 7.



```
root@kali: ~/investigasi
File  Actions  Edit  View  Help

┌──(root㉿kali)-[~/investigasi]
└─# foremost -i bukti.dd -o foremost -v
Foremost version 1.5.7 by Jesse Kornblum, Kris Kendall, and Nick Mikus
Audit File

Foremost started at Mon Jun 12 03:00:09 2023
Invocation: foremost -i bukti.dd -o foremost -v
Output directory: /root/investigasi/foremost
Configuration file: /etc/foremost.conf
Processing: bukti.dd
|----------------------------------------------------------------
File: bukti.dd
Start: Mon Jun 12 03:00:09 2023
Length: 7 GB (8000634880 bytes)

Num      Name (bs=512)          Size       File Offset      Comment

0:      00032847.jpg           6 KB         16817931
1:      00032860.jpg           6 KB         16824803
```

Figure 7. The process of returning carving files uses foremost

Figure 7 shows the Foremost software recovering and reconstructing the files found in the cloned files. This process allows the investigator to collect evidence relevant to the investigated case. The time taken to perform the data recovery process using Foremost is 1 minute and 3 seconds. In addition, the data recovery process was also carried out using Scalpel software, as shown in Figure 8.



```
┌──(root㉿kali)-[~]
└─# cd investigasi

┌──(root㉿kali)-[~/investigasi]
└─# scalpel bukti.dd -o scalpel -v
Scalpel version 1.60
Written by Golden G. Richard III, based on Foremost 0.69.
Output directory: "/root/investigasi/scalpel"
Configuration file: "/etc/scalpel/scalpel.conf"
Coverage maps directory: "/root/investigasi/scalpel"

Opening target "/root/investigasi/bukti.dd"

Total file size is 8000634880 bytes
Image file pass 1/2.
Read 10485760 bytes from image file.
bukti.dd:   0.1% |                                                    |   10.0 MB
Read 10485760 bytes from image file.
bukti.dd:   0.3% |                                                    |   20.0 MB
A jpg header was found at : 16817931
Memory reallocation performed, total header storage = 101
A jpg header was found at : 16824803
```

Figure 8. The process of returning carving files uses scalpel

Figure 8 shows the file carving process using Scalpel software, aimed at finding and collecting pieces of files that may be fragmented or deleted from the cloned data. Using pre-configured custom patterns, Scalpel can identify and recover evidence in the cloned data. The time required to perform the data recovery process using Scalpel is 2 minutes and 17 seconds. By using Foremost and Scalpel software together, investigators can thoroughly examine the cloned data and obtain important and relevant evidence in the investigated data theft case.

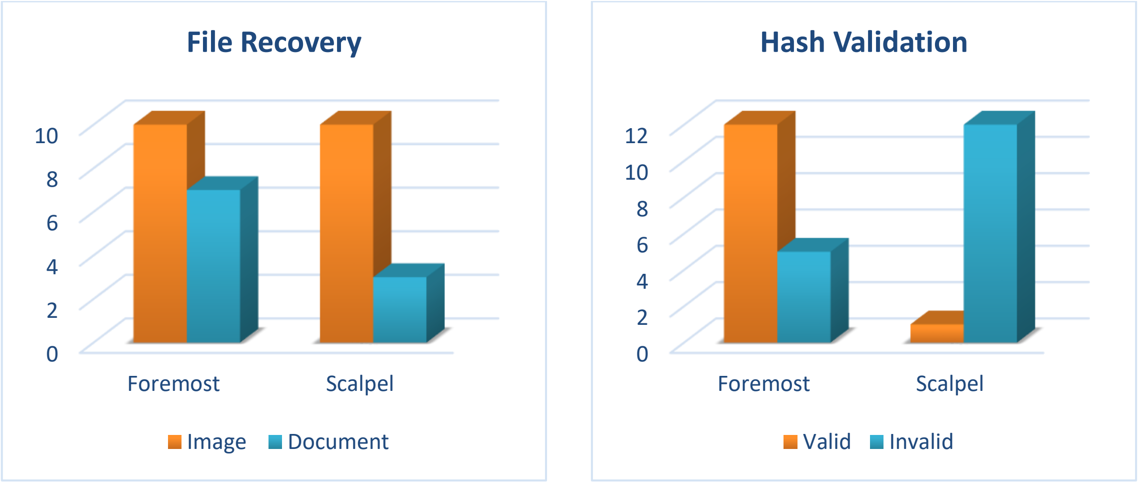
Analysis

After successfully locating the files resulting from the file carving process, the investigator will analyze the content and metadata of the deleted PDF and JPG files. The extracted data will be analyzed by examining the file structure, associated metadata, and content of the files found through the file carving process. The analysis process is dominated by an advanced investigation based on parameters set as evidence. This evidence will become strong digital evidence and can be used in the disclosure process of the case. The following Table 4 shows artifact extraction and digital evidence validation results.

Table 4. Evidence found and validation of the hash values

No	Evidence Name			File Type	Evidence Found		Hash Value Validation	
	Original	Foremost	Scalpel		Foremost	Scalpel	Foremost	Scalpel
1	Data 1	00032960	00000005	.jpg	✓	✓	✓	X
2	Data 2	00033416	00000006	.jpg	✓	✓	✓	X
3	Data 3	00033856	00000007	.jpg	✓	✓	✓	X
4	Data 4	00034312	00000008	.jpg	✓	✓	✓	X
5	Data 5	00034648	00000009	.jpg	✓	✓	✓	X
6	Data 6	00035104	00000010	.jpg	✓	✓	✓	X
7	Data 7	00035560	00000011	.jpg	✓	✓	✓	X
8	Data 8	00035976	00000012	.jpg	✓	✓	✓	X
9	Data 9	00036392	00000013	.jpg	✓	✓	✓	X
10	Data 10	00036816	00000014	.jpg	✓	✓	✓	X
11	Data 11	00032800	-	.pdf	✓	-	X	-
12	Data 12	00038224	-	.pdf	✓	-	✓	-
13	Data 13	00038624	-	.pdf	✓	-	X	-
14	Data 14	00040160	00000036	.pdf	✓	✓	X	✓
15	Data 15	-	00000022	.pdf	-	✓	-	X
16	Data 16	00041288	-	.pdf	✓	-	✓	-
17	Data 17	-	-	.pdf	-	-	-	-
18	Data 18	00043592	-	.pdf	✓	-	X	-
19	Data 19	00044008	00000023	.pdf	✓	✓	X	X
20	Data 20	-	-	.pdf	-	-	-	-

Table 4 shows that Foremost software successfully found 17 carving files, but five files had invalid hash codes. Meanwhile, Scalpel software successfully found 13 carved files, but 12 files showed invalid hash values. A graphic visualization of the number of successfully recovered files and hash value validation can be seen in in the following Figure 9.



(a) Graph of file carving results (b) Graph of hash validation results

Figure 9. Graph of Foremost and Scalpel hash recovery and validation results

Based on Figure 9 (a), the next step is to measure the accuracy index to assess the ability of each tool to restore the carved file. This measurement can be calculated using the formula in Equation (2) and Equation (3), established by [52].

Foremost tool:

$$Par = \frac{\sum 17}{\sum 20} \times 100\ \% = 85\% \tag{2}$$

Scalpel tool:

$$Par = \frac{\sum 13}{\sum 20} \times 100\ \% = 65\% \tag{3}$$

The results of the digital evidence tool comparison show that the Foremost forensic tool has a better file carving return rate than Scalpel. Foremost achieved an accuracy index of 85%, while Scalpel only achieved an accuracy index of 65%. Afterward, an accuracy index measurement is performed to measure the ability of each tool to achieve identical hash values based on Figure 9 (b). This calculation uses the formula [52] in Equation (4) and Equation (5).

Foremost tool:

$$Par = \frac{\sum 12}{\sum 17} \times 100\ \% = 70.59\% \tag{4}$$

Scalpel tool:

$$Par = \frac{\sum 1}{\sum 13} \times 100\ \% = 7.69\% \tag{5}$$

The comparison results show that the Foremost forensic tool has an identical hash value index of 70.59%, while the Scalpel software only has an identical hash value index of 7.69%.

Presentation

The results of the digital forensic evidence analysis stages in the scenario of company data theft cases can be compared using three parameters: the speed of the recovery process, the number of files successfully recovered, and the correctness of the recovered files. A comparison of the results of digital evidence based on the capabilities of forensic tools is presented in following table.

Table 5. Forensic tool comparison results

No	Forensic Tool Name	Recovery Time	Recovery Rate	Identical Hash Values
1	Foremost	1 Minute 3 Seconds	85%	70.59%
2	Scalpel	2 Minute 17 Seconds	65%	7.69%

Table 5 presents the simulation results and scenario analysis based on the DFRWS forensic stages on Flash disk storage media. These results show that the Foremost forensic tool quickly recovered the data within 1 minute and 3 seconds. Data recovery accuracy reached 85%, while the similarity of hash values reached 70.59%.

Discussion

Based on the comparative analysis and evaluation of the ability of file carving tools in handling digital crime cases on Flash disk storage media by applying the DFRWS method, evidence was found in the form of files in jpg and pdf formats. Foremost is the best file carving tool, with a success rate of 85% and an identical hash value match of 70.59%. In addition, Foremost is also faster in the acquisition process compared to Scalpel. This research contributes to the field of cybercrime involving the use of Flash disk as storage media and can be a reference for investigators regarding the best file carving tool. The results of this research also compare with previous research related to the DFRWS framework in handling digital evidence, as shown in the following Table 6.

Table 6. Comparison of previous research using DFWRS framework method

References	Method	Type of evidence	Forensic tools	Recovery Rate	Results
[47]	DFWRS	Secure Digital	Foremost	77%	Foremost can be used in digital forensics for Secure Digital High Capacity.
[48]	DFWRS	Signal Messenger Application	Belkasoft Evidence Center Magnet AXIOM MOBILedit Forensic Express	78.69% 26.23% 9.84%	Belkasoft Evidence Center is the best tool for handling digital forensics in the Signal Messenger application.
[49]	DFWRS	Smartphone	Oxygen Forensic	90%	Oxygen Forensic can be used in Audio Forensics on Smartphones.
[50]	DFWRS	Instagram Applications	Magnet Axiom Cellebrite UFED	87.5% 68.75%	Magnet Axiom is the best tool to overcome cases of spreading hoax news on the Instagram application.
This research	DFWRS	Flash disk	Foremost Scalpel	85% 65%	Foremost is the best tool for handling digital forensics on Flash disk.

Table 6 shows a comparison of various forensic tools and methods used in digital data recovery. This table illustrates the advantages and disadvantages of each forensic tool and method in various digital forensic scenarios.

CONCLUSION

This research successfully applies the DFRWS framework to investigate the crime of theft of confidential company data that has been deleted from Flash disk storage media. The data acquisition process using DC3DD software produces digital evidence with the same hash value as the original file. The results of this study show that Foremost software successfully recovered the carving file in 1 minute 3 seconds with an accuracy rate of 85% and an identical hash value rate of 70.59%. Meanwhile, Scalpel software recovered the carving file in 2 minutes 17 seconds with an accuracy rate of 65% and an identical hash value rate of 7.69%. The results of the comparison of these two software tools show that Foremost is superior to Scalpel, so it is recommended for use in the process of acquiring digital evidence on Flash disk storage media.

REFERENCES

[1] F. Lathifah and A. Fadhil Musyaffa, “Performance and quality measurement of internet network services at muhammadiyah university of surakarta’s faculty of health sciences with QOS parameter,” *J. Student Res. Explor.*, vol. 1, no. 2, pp. 64–72, Mar. 2023, doi: 10.52465/josre.v1i2.148.

[2] D. A. A. Pertiwi, M. Yusuf, and D. A. Efrilianda, “Operational Supply Chain Risk Management on Apparel Industry Based on Supply Chain Operation Reference (SCOR),” *J. Inf. Syst. Explor. Res.*,

vol. 1, no. 1, pp. 17–24, Dec. 2022, doi: 10.52465/joiser.v1i1.103.

[3] “Factors affecting interest in utilization and use of online shop (study on shopee customers),” *J. Soft Comput. Explor.*, vol. 2, no. 2, Sep. 2021, doi: 10.52465/joscex.v2i2.45.

[4] G. T. Siregar and S. Sinaga, “The Law Globalization in Cybercrime Prevention,” *Int. J. Law Reconstr.*, vol. 5, no. 2, pp. 211–227, Sep. 2021, doi: 10.26532/ijlr.v5i2.17514.

[5] G. Cascavilla, D. A. Tamburri, and W.-J. Van Den Heuvel, “Cybercrime threat intelligence: A systematic multi-vocal literature review,” *Comput. Secur.*, vol. 105, p. 102258, Jun. 2021, doi: 10.1016/j.cose.2021.102258.

[6] A. Okutan and Y. Çebi, “A Framework for Cyber Crime Investigation,” *Procedia Comput. Sci.*, vol. 158, pp. 287–294, 2019, doi: 10.1016/j.procs.2019.09.054.

[7] D. Buil-Gil, F. Miró-Llinares, A. Moneva, S. Kemp, and N. Díaz-Castaño, “Cybercrime and shifts in opportunities during COVID-19: a preliminary analysis in the UK,” *Eur. Soc.*, vol. 23, no. S1, pp. S47–S59, 2021, doi: 10.1080/14616696.2020.1804973.

[8] W. A. Al-Khater, S. Al-Maadeed, A. A. Ahmed, A. S. Sadiq, and M. K. Khan, “Comprehensive review of cybercrime detection techniques,” *IEEE Access*, vol. 8, pp. 137293–137311, 2020, doi: 10.1109/ACCESS.2020.3011259.

[9] P. Siber, “Jumlah Laporan Polisi yang dibuat masyarakat,” *Patroli Siber*, 2023.

[10] Y. Li and Q. Liu, “A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments,” *Energy Reports*, vol. 7, pp. 8176–8186, 2021, doi: 10.1016/j.egyr.2021.08.126.

[11] S. Chng, H. Y. Lu, A. Kumar, and D. Yau, “Hacker types, motivations and strategies: A comprehensive framework,” *Comput. Hum. Behav. Reports*, vol. 5, p. 100167, 2022, doi: 10.1016/j.chbr.2022.100167.

[12] T. U. Rehman, S. Parveen, M. A. Usmani, and M. A. Y. Khan, “Varieties and Skills of Cybercrime,” *Int. J. Cyber Behav. Psychol. Learn.*, vol. 13, no. 1, pp. 1–13, 2023, doi: 10.4018/IJCBPL.324091.

[13] A. Mishra, Y. I. Alzoubi, M. J. Anwar, and A. Q. Gill, “Attributes impacting cybersecurity policy development: An evidence from seven nations,” *Comput. Secur.*, vol. 120, p. 102820, Sep. 2022, doi: 10.1016/j.cose.2022.102820.

[14] M. Javaid, A. Haleem, R. P. Singh, and R. Suman, “Towards insighting cybersecurity for healthcare domains: A comprehensive review of recent practices and trends,” *Cyber Secur. Appl.*, vol. 1, no. August 2022, p. 100016, Dec. 2023, doi: 10.1016/j.csa.2023.100016.

[15] M. I. Al-Saleh and M. J. Al-Shamaileh, “Forensic artefacts associated with intentionally deleted user accounts,” *Int. J. Electron. Secur. Digit. Forensics*, vol. 9, no. 2, pp. 167–179, 2017, doi: 10.1504/IJESDF.2017.083992.

[16] K. Conlan, I. Baggili, and F. Breitinger, “Anti-forensics: Furthering digital forensic science through a new extended, granular taxonomy,” *Digit. Investig.*, vol. 18, pp. S66–S75, Aug. 2016, doi: 10.1016/j.diin.2016.04.006.

[17] S. Nazah, S. Huda, J. Abawajy, and M. M. Hassan, “Evolution of dark web threat analysis and detection: A systematic approach,” *IEEE Access*, vol. 8, pp. 171796–171819, 2020, doi: 10.1109/ACCESS.2020.3024198.

[18] A. Kazim, F. Almaeeni, S. Al Ali, F. Iqbal, and K. Al-Hussaeni, “Memory Forensics: Recovering Chat Messages and Encryption Master Key,” *2019 10th Int. Conf. Inf. Commun. Syst. ICICS 2019*, pp. 58–64, 2019, doi: 10.1109/IACS.2019.8809179.

[19] K. Shaukat, S. Luo, V. Varadharajan, I. A. Hameed, and M. Xu, “A Survey on Machine Learning Techniques for Cyber Security in the Last Decade,” *IEEE Access*, vol. 8, pp. 222310–222354, 2020, doi: 10.1109/ACCESS.2020.3041951.

[20] S. Gupta Bhol, J. R. Mohanty, and P. Kumar Pattnaik, “Taxonomy of cyber security metrics to measure strength of cyber security,” *Mater. Today Proc.*, vol. 80, pp. 2274–2279, 2023, doi: 10.1016/j.matpr.2021.06.228.

[21] A. Hamid, M. Alam, H. Sheherin, and A. S. K. Pathan, “Cyber security concerns in social networking service,” *Int. J. Commun. Networks Inf. Secur.*, vol. 12, no. 2, pp. 198–212, 2020, doi: 10.17762/ijcnis.v12i2.4634.

[22] N. Chen and B. Chen, “Defending against OS-Level Malware in Mobile Devices via Real-Time Malware Detection and Storage Restoration,” *J. Cybersecurity Priv.*, vol. 2, no. 2, pp. 311–328, 2022, doi: 10.3390/jcp2020017.

[23] F. Faghihi and M. Zulkernine, “RansomCare: Data-centric detection and mitigation against smartphone crypto-ransomware,” *Comput. Networks*, vol. 191, p. 108011, 2021, doi: 10.1016/j.comnet.2021.108011.

[24] N. U. Richards and F. E. Eboibi, “African governments and the influence of corruption on the proliferation of cybercrime in Africa: wherein lies the rule of law?,” *Int. Rev. Law, Comput. Technol.*, vol. 35, no. 2, pp. 131–161, 2021, doi: 10.1080/13600869.2021.1885105.

[25] I. Cunha, J. Cavalcante, and A. Patel, “A proposal for curriculum development of educating and training Brazilian police officers in digital forensics investigation and cybercrime prosecution,” *Int. J. Electron. Secur. Digit. Forensics*, vol. 9, no. 3, pp. 209–238, 2017, doi: 10.1504/IJESDF.2017.085195.

[26] R. I. Ferguson, K. Renaud, S. Wilford, and A. Irons, “PRECEPT: a framework for ethical digital forensics investigations,” *J. Intellect. Cap.*, vol. 21, no. 2, pp. 257–290, 2020, doi: 10.1108/JIC-05-2019-0097.

[27] R. R. Ali, K. M. Mohamad, S. Jamel, and S. K. A. Khalid, “A review of digital forensics methods for JPEG file carving,” *J. Theor. Appl. Inf. Technol.*, vol. 96, no. 17, pp. 5841–5856, 2018.

[28] K. Ghazinour, D. M. Vakharia, K. C. Kannaji, and R. Satyakumar, “A study on digital forensic tools,” *IEEE Int. Conf. Power, Control. Signals Instrum. Eng. ICPCSI 2017*, pp. 3136–3142, 2018, doi: 10.1109/ICPCSI.2017.8392304.

[29] K. Alghafli, C. Y. Yeun, and E. Damiani, “Techniques for Measuring the Probability of Adjacency between Carved Video Fragments: The VidCarve Approach,” *IEEE Trans. Sustain. Comput.*, vol. 6, no. 1, pp. 131–143, 2021, doi: 10.1109/TSUSC.2019.2914192.

[30] P. Gladyshev and J. I. James, “Decision-theoretic file carving,” *Digit. Investig.*, vol. 22, pp. 46–61, 2017, doi: 10.1016/j.diin.2017.08.001.

[31] M. F. Abdillah and Y. Prayudi, “Data Recovery Comparative Analysis using Open-based Forensic Tools Source on Linux,” *Int. J. Adv. Comput. Sci. Appl.*, vol. 13, no. 9, pp. 633–639, 2022, doi: 10.14569/IJACSA.2022.0130975.

[32] U. Karabiyik and T. Karabiyik, “A game theoretic approach for digital forensic tool selection,” *Mathematics*, vol. 8, no. 5, pp. 1–13, 2020, doi: 10.3390/MATH8050774.

[33] A. K. Pratama, C. Carudin, and D. Yusup, “Analisis Perbandingan Perangkat Lunak Forensik Digital untuk File Carving dalam Mengungkap Barang Bukti Digital,” *JUSTINDO (Jurnal Sist. dan Teknol. Inf. Indones.*, vol. 6, no. 2, pp. 109–120, 2021, doi: 10.32528/justindo.v6i2.5101.

[34] S. Soni, Y. Fatma, and R. Anwar, “Akuisisi Bukti Digital Aplikasi Pesan Instan ‘Bip’Menggunakan Metode National Institute Of Justice (NIJ),” *J. CoSciTech (Computer Sci. Inf. Technol.*, vol. 3, no. 1, pp. 34–42, 2022, doi: 10.37859/coscitech.v3i1.3694.

[35] I. Riadi, S. Sunardi, and M. E. Rauli, “Live Forensics Analysis of Line App on Proprietary Operating System,” *Kinet. Game Technol. Inf. Syst. Comput. Network, Comput. Electron. Control*, vol. 4, no. 3, pp. 305–314, Oct. 2019, doi: 10.22219/kinetik.v4i4.850.

[36] R. N. Bintang, R. Umar, and A. Yudhana, “Assess of Forensic Tools on Android Based Facebook Lite with the NIST Method,” *Sci. J. Informatics*, vol. 8, no. 1, pp. 1–9, 2021, doi: 10.15294/sji.v8i1.26744.

[37] I. Riadi, A. Yudhana, and M. C. F. Putra, “Forensic Tool Comparison on Instagram Digital Evidence Based on Android with The NIST Method,” *Sci. J. Informatics*, vol. 5, no. 2, pp. 235–247, 2018, doi: 10.15294/sji.v5i2.16545.

[38] R. Umar, I. Riadi, and B. F. Muthohirin, “Live forensics of tools on android devices for email forensics,” *Telkomnika (Telecommunication Comput. Electron. Control.*, vol. 17, no. 4, pp. 1803–1809, 2019, doi: 10.12928/TELKOMNIKA.v17i4.11748.

[39] A. Yudhana, R. Umar, and A. Ahmadi, “Digital Evidence Identification on Google Drive in Android Device Using NIST Mobile Forensic Method,” *Sci. J. Informatics*, vol. 6, no. 1, pp. 54–63, 2019, doi: 10.15294/sji.v6i1.17767.

[40] Herman, I. Riadi, and I. A. Rafiq, “Forensic Mobile Analysis on Social Media Using National Institute Standard of Technology Method,” *Int. J. Saf. Secur. Eng.*, vol. 12, no. 6, pp. 707–713, 2022, doi: 10.18280/ijsse.120606.

[41] I. Riadi, Sunardi, and P. Widiandana, “Investigating Cyberbullying on WhatsApp Using Digital Forensics Research Workshop,” *J. RESTI (Rekayasa Sist. dan Teknol. Informasi)*, vol. 4, no. 4, pp. 730–735, 2020, doi: 10.29207/resti.v4i4.2161.

[42] I. Zuhriyanto, A. Yudhana, and I. Riadi, “Comparative analysis of Forensic Tools on Twitter applications using the DFRWS method,” *J. RESTI (Rekayasa Sist. dan Teknol. Informasi)*, vol. 4, no. 5, pp. 829–836, Oct. 2020, doi: 10.29207/resti.v4i5.2152.

[43] I. Riadi, H. Herman, and N. H. Siregar, “Mobile Forensic of Vaccine Hoaxes on Signal Messenger using DFRWS Framework,” *MATRIK J. Manajemen, Tek. Inform. dan Rekayasa Komput.*, vol. 21, no. 3, pp. 489–502, 2022, doi: 10.30812/matrik.v21i3.1620.

[44] R. Y. Prasongko, A. Yudhana, and I. Riadi, “Analysis of the Use of the ACPO (Association of Chief Police Officer) Method in WhatsApp Forensics,” *J. Sains Komput. Inform. (J-SAKTI*, vol. 6, no. 2, pp. 1112–1120, 2022, doi: 10.30645/j-sakti.v6i2.520.

[45] Sunardi, Imam Riadi, and Muh. Hajar Akbar, “Application of Static Forensics Method for Extracting Steganographic Files on Digital Evidence Using the DFRWS Framework,” *J. RESTI (Rekayasa Sist. dan Teknol. Informasi)*, vol. 4, no. 3, pp. 576–583, Jun. 2020, doi: 10.29207/resti.v4i3.1906.

[46] J. N. Hilgert, M. Lambertz, M. Rybalka, and R. Schell, “Syntactical Carving of PNGs and Automated Generation of Reproducible Datasets,” *Digit. Investig.*, vol. 29, pp. S22–S30, 2019, doi: 10.1016/j.diin.2019.04.014.

[47] A. Yudhana, Imam Riadi, and Budi Putra, “Digital Forensic on Secure Digital High Capacity using DFRWS Method,” *J. RESTI (Rekayasa Sist. dan Teknol. Informasi)*, vol. 6, no. 6, pp. 1021–1027, Dec. 2022, doi: 10.29207/resti.v6i6.4615.

[48] I. Riadi, Herman, and N. H. Siregar, “Mobile Forensic Analysis of Signal Messenger Application on Android using Digital Forensic Research Workshop (DFRWS) Framework,” *Ingénierie des systèmes d Inf.*, vol. 27, no. 6, pp. 903–913, Dec. 2022, doi: 10.18280/isi.270606.

[49] S. Sunardi, I. Riadi, R. Umar, and M. F. Gustafi, “Audio Forensics on Smartphone with Digital Forensics Research Workshop (DFRWS) Method,” *CommIT (Communication Inf. Technol. J.*, vol. 15, no. 1, pp. 41–47, Mar. 2021, doi: 10.21512/commit.v15i1.6739.

[50] I. Riadi, H. Herman, and I. A. Rafiq, “Mobile Forensic Investigation of Fake News Cases on Instagram Applications with Digital Forensics Research Workshop Framework,” *Int. J. Artif. Intell. Res.*, vol. 6, no. 2, Jul. 2022, doi: 10.29099/ijair.v6i2.311.

[51] A. Yudhana, I. Riadi, and R. Y. Prasongko, “Forensik WhatsApp Menggunakan Metode Digital Forensic Research Workshop (DFRWS),” *J. Inform. J. Pengemb. IT*, vol. 7, no. 1, pp. 43–48, 2022, doi: 10.30591/jpit.v7i1.3639.

[52] R. Umar, A. Yudhana, and M. N. Fadillah, “Perbandingan Tools Forensik pada Aplikasi Dompet Digital,” *JIKO (Jurnal Inform. dan Komputer)*, vol. 6, no. 2, pp. 242–250, Sep. 2022, doi: 10.26798/jiko.v6i2.621.

[53] M. H. Akbar, S. Sunardi, and I. Riadi, “Steganalysis Bukti Digital pada Media Storage Menggunakan Metode GCFIM,” *JISKA (Jurnal Inform. Sunan Kalijaga)*, vol. 5, no. 2, pp. 96–106, Sep. 2020, doi: 10.14421/jiska.2020.52-04.