Accredited Ranking SINTA 2
Decree of the Director General of Higher Education, Research, and Technology, No. 158/E/KPT/2021
Validity period from Volume 5 Number 2 of 2021 to Volume 10 Number 1 of 2026

Published online on: **http://jurnal.iaii.or.id**

JURNAL RESTI
(Rekayasa Sistem dan Teknologi Informasi)
Vol. 6 No. x (2022) 1021-1027 ISSN Media Electronic: 2580-0760

Digital Forensic on Secure Digital High Capacity using DFRWS Method

Anton Yudhana[1], Imam Riadi[2], Budi Putra[3]
[1]Department of Electrical Engineering, Universitas Ahmad Dahlan
[2]Department of Information System, Universitas Ahmad Dahlan
[3]Department of Informatics, Universitas Ahmad Dahlan,
[1]eyudhana@ee.uad.ac.id [2]imam.riadi@is.uad.ac.id [3]budi1808048034@webmail.uad.ac.id*

Abstract

As evidenced in the trial, between 2015 and the second quarter of 2022, there were 54 cases involving secure digital high capacity (SDHC) storage hardware as evidenced in trials. In 2021 there will be an increase in cases involving SDHC. The three cases with the highest number are corruption cases, special crimes, and ITE. SDHC is an advanced technology development of Secure Digital (SD) card hardware which functions as storage. SD Card only has a capacity of up to 2 gigabytes, while the largest SDHC capacity is 32 gigabytes. As a storage device that is small, thin, and has a fairly large capacity. this research needs to be done because of the increasingly widespread increase in cases involving SDHC. This study aims to perform digital forensic analysis on SDHC evidence using forensic applications that run on Linux, namely foremost and DC3DD. This study uses the DFRWS method to retrieve valid evidence in court. Based on the research conducted, it was found that the number of files that can be restored at the examination stage using foremost is 77%, and the accuracy of recovered files is 50% with string file hash validation. From this research, it can be concluded that the processing results of DC3DD and Foremost can be used as valid evidence.

Keywords: Digital forensic, sdhc, dfrws, linux, foremost, dc3dd

1. Introduction

From 2015 to the second quarter of 2022, there were 54 cases involving secure digital high capacity (SDHC) storage hardware as evidence in the trial, according to the records of the supreme court's decision as presented in Figure 1. The spike occurred in 2021; if classified, there are three cases with the highest number of corruption cases, exceptional criminal cases and ITE cases[1]. One of these cases involved the defendant with the initials AUS.

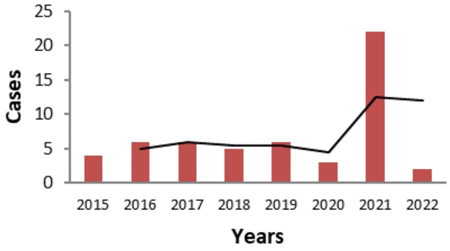


Figure 1. Case Evidence Involing SDHC

The case has a decision number 43/PID.TPK/2021/PT BDG 2022. The defendant with the initials AUS committed a particular crime of corruption. As a result of the case, AUS was threatened with seven years in prison and a fine of Rp. 300,000,000,- (three hundred million rupiahs)[2], the digital evidence, in this case, is in the form of 5 files presented in Table 1; there are various types of file extensions stored on SDHC, namely three compressed files in .zip format and two database files ad1 format, The entire file was in one of the confiscated evidence, namely the defendant's SDHC storage card.

Table 1. File on SDHC

File Name	Hash MD5
“Surat Keluar dan Masuk Bupati KBB(R Sekpri).zip”	3154cb3b302640568 b29fe64fe883b6a
“Document Komputer Pak Agus Pribadi (R Asisten II EKBANG).zip IP Address LPSE.xlsx.zip”	325ff9abf462bebda03 7c23d8b81b6c6 ada844879277a76970 d2976be9e7a2ad
“202103161711.ad1”	1f4e721963b701916f 156d809d97ff6d
"202103171512.ad1"	994174d1834894fd85 c7be42f03c5e4e

SDHC storage cards are hardware with an architecture that has similarities with other types of memory cards, namely monolithic[3]; SDHC is a further development of Secure Digital (SD) card storage hardware which can only accommodate up to a capacity of 2 gigabytes, in contrast to the largest SD card capacity. SDHC-type

Accepted: 26-10-2022 | Received in revised: 16-12-2022 | Published: 29-12-2022

memory card is 32 gigabytes[4]; based on this capability, not all devices can use SDHC; as a small, thin and large storage device[5], SDHC storage hardware is a minimalist and multifunctional storage device, as shown in the Figure. 2. In cases involving AUS, the data on SDHC can be deleted, transferred or changed; the data is required to verify the authenticity of digital evidence with a digital forensic process.

Figure 2. Physical Interface SDHC

Digital forensics is a scientific effort to recover and investigate material against digital evidence[6]; digital forensics aims to provide choices and recommendations to judges to uncover a criminal case (pro-justice)[7]; the digital forensic process needs to be carried out with measurable and structured steps, various framework methods are commonly used, some of which include the Digital Forensics Research Workshop (DFRWS)[8], Association of Chief Police Officers (ACPO)[9], National Institute of Justice (NIJ)[10], Institute Of Standards And Technology (NIST)[11], Digital Forensic Investigation Framework (IDFIF) V2[12], in general, the method begins with steps of maintenance, validation, collection, analysis, identification, documentation, interpretation and presentation of digital evidence so that valid evidence is obtained based on the facts strung from the digital evidence investigation process[13].

Digital evidence is not only intended for cyber crimes but can be used for all types of crimes[14]. Digital evidence can result from the extraction or recovery of digital goods, for example, files, email accounts, contacts, documents, photos, videos, images, chat text and log files[15]. The results obtained from the evidence analysis will vary according to the case being worked on. The handling of digital evidence must be handled properly because it is vulnerable and easy to change if not appropriately treated[16]; whatever changes occur in digital evidence will result in the evidence being invalid in court[17]. In the process of processing evidence. there are various platforms that can be used, one of which is Linux.

Linux is an operating system that has a different hierarchy and way of working from other proprietary operating systems[18], but only a few software are capable of running on the Linux operating system, because the operating system is open source and free of charge according to the license[19]. can run on a linux operating system, namely DC3DD which functions to perform acquisitions and software. Most importantly, which aims to perform data carving[20].

Hash or hashing is an algorithm to check the originality of a file[21]. Hashing technique is an act of changing a process to change another data with the same value so that the data cannot be recovered[22]. In other words, the hash is a fingerprint of a file[23]. Every file must have different fingerprints. Hash checks for file validation are carried out after carving data on evidence. There are several types of hashes that are often used, including the SHA-1 and MD5 algorithm[24].

Based on previous literature studies using similar objects, the results of the research conclude that image carving using FTK Imager and Autopsy by Shift+Delete and wipe data have image carving results on shift+delete that are still able to be recovered. Recovery results only get residual files in the image carving process with the wipe model data[25].

Previous research only carried out the acquisition and analysis of evidence using paid forensic tools for proprietary operating systems without a standardized framework. In this study, digital forensics was carried out on SDHC storage media and used Linux-based or open-source forensic tools, namely foremost and dc3dd; this research uses the DFRWS framework method and the static forensic process to retrieve valid digital evidence so that it can be used as legal evidence and can be understood by investigators when solving similar crimes.

This study aims to perform digital forensic analysis on SDHC evidence using forensic applications running on Linux, namely foremost and DC3DD. This study uses the DFRWS method to retrieve evidence for legal evidence in the trial.

2. Research Methods

In this study, the Digital forensic research workshop (DFRWS) method was chosen to be used as a framework. The DFRWS method has a framework accompanied by several steps or a digital forensic investigation process, as shown in Figure 3.

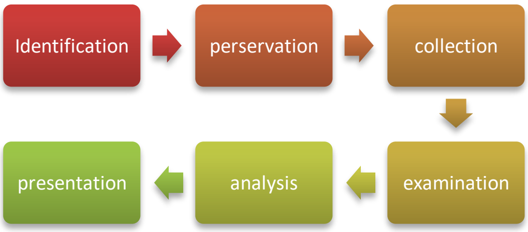


Figure 3. Step of DFRWS Method

Figure 3 describes the sequence of steps or the investigation process with the DFRWS framework that will be used to carry out an investigative action. The first step is identification; in the identification step, an in-depth examination process is carried out to determine the needs of the investigation and evidence carried out by the investigator[26]. The second step is preservation; in this step, the protection of the evidence is carried out so that the evidence is protected from unauthorized parties and also ensures the authenticity of the evidence[27]. The next step is the collection; at this step, evidence is preserved so that it can be ascertained that the evidence is genuine; if there is a change in the evidence, then the evidence is invalid/valid to be submitted at the trial[28].

The fourth step is an examination; at this step, an examination of the evidence taken during collection and a search for digital evidence that can potentially become strong evidence and recovery of digital evidence is carried out[29]. The next step is analysis. In this process, digital evidence is validated so that digital evidence can be declared valid/valid when submitted[30]. The last step is presentation. This step is a process of presenting the results of information in detail, detail and informative[31].

2.1 Case Simulation

In this study, evidence was obtained through case simulations, not based on actual events. Figure 4 shows a case simulation which is an artificial scenario.

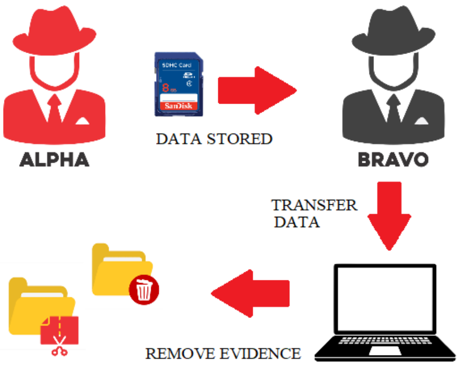


Figure 4. Simulation of Mafia Data Transfer Cases

Figure 4 illustrates a case simulation starting from the existence of a mafia organization in a city in Indonesia, one of the members has the title Alpha and is in charge of collecting information and data on assets owned by the organization. These data are stored in the organization's activities through an SDHC storage media. After Performing its duties, Alpha will hand it over to Bravo, who is in charge of maintaining the information and data. After receiving the SDHC, Bravo will sort the files through the cut process (CTRL+X) and delete (Delete) to select files and remove digital evidence from SDHC to the main computer. Investigators found SDHC, which was indicated as electronic evidence of the case.

2.2 Equipment and Materials

The equipment and materials used in this study are presented in Table 2.

Table 2. List of Equipment dan Materials

Equipment	Specification	Description
Notebook	Lenovo G40, Intel i5, DDR3	Hardware
Operation System	Ubuntu 22.04 64bit	Software
DC3DD	Ver 7.2 64 bit	Imaging Forensic Software
Foremost	Ver 1.5.7	Forensic Software
Sandisk SDHC	16 GB	Hardware

Details of the authenticity of the files that will be tested in this study are separated into two folders, each file is taken its hash value before doing case simulation, later the hash will be matched on the file that has been recovered, the first folder files contained can be seen in Table 3. All files contained in this folder will be deleted using (delete), There are various file extensions used in the case simulation in this study included .exe, .jpg, .pdf, .mov, .rar, and .word, the number that represents each extension is 3 files so that later it will be easier to calculate the results.

Table 3. Index of First Folder and SHA1 hash

File Name	Hash SHA-1
file exe (1)	de3dce853c08b385d43822aaafc55d1e19f6055f
file exe (2)	73b387f9e43641a9d62e675afb97eb82075d6e53
file exe (3)	934204df9af6cb55de6be4f404033d233f80a14b
file gambar (1)	53430ae10506878724ac7921aba667375fd4ea17
file gambar (2)	573386b9dbdb09d16d5b91080a95b82a5de2e693
file gambar (3)	254172bf6bb9da169cfb33ef419b93be79aa5033
file pdf (1)	ccae3c8fae6092ce2c32aa27676f341c29374f8a
file pdf (2)	faced5a3520ee2c316556ff937c755439712af73
file pdf (3)	d4f5ef5d26c9ef65f53e70c8e4fc6128348ae084
filevideo (1)	5100e5d2d7f943ce43d0efb02008d90b072a8218
filevideo (2)	4c1538f29814a43306a2fe0851f6f05d66e8341b
filevideo (3)	964c9e9086d6587964669ccb268e71c6dc6cd0bd
file winrar (1)	15c5c5db4d667df80b76822053b72fb11713cde8
file winrar (2)	489e5b8ffcc090cc93039b5dcbb262413b054609
file winrar (3)	37e05a023e0237dd66427b367812d91dca1090a9
file word (1)	79e5e711033faba7cda3b7aa199d1be1397f4aba
file word (2)	203c78257b05794cc6ad0dea985fffeb600a0295
file word (3)	f5c2ef463e8c999e93d195e91ad925b7b6013c54

Table 4. Index of Second Folder and SHA-1 hash

File Name	Hash SHA-1
file exe (4)	ab340f9bc86e31d1d4d8440875d1bffafe10346d
file exe (5)	0ac9d87b592b332924c77613d65a7a47d46cf259
file exe (6)	cbc27981351558117a75e37aa6dbd24064e2ca07
file gambar (4)	b6795c746195f81fdf863b8babb33b0920edbcf1
file gambar (5)	2f15eccf8ac7bc8c453aea277eceb4d93cfc26a9
file gambar (6)	1d25b1e40a381ba82afe5f02247a952739eeea4a
file pdf (4)	7ec31dd4699627ef3ff5f060a6eabfb214876c1c
file pdf (5)	e1a40c0757dbf7e0efa97c6bd3dd97cac292bec7
file pdf (6)	99e98168cbf486fe3faab0b45372a79bf1992da3
filevideo (4)	c952307a2ca41ba98be7e87b8a07b3f8b124110e
filevideo (5)	db2354c74550cd33b124997e1b0045f6bcb5e123
filevideo (6)	da34d973a998a7bcb9d675938b94efcd7d9a5a87
file winrar (4)	aaa1735e8ba0f9b3eb3ec33c2382f8ec44e42444
file winrar (5)	73dc18aec8e692638fd51f7af7bfaa3fc749d79b
file winrar (6)	9623bccfd9b2c96145810d74ba9ebcde216a17d3
file word (4)	4b9359733b3a7645e41201a76e0c52e0c7638e68
file word (5)	1a11e580f0b901cd987fb6e85668bc23565e3cdf
file word (6)	a9dbf91a4176db2a2ad7a78c779c3a932e2b9d82

The files contained in the second folder can be seen in Table 4. All files contained in this folder will be moved by (Ctrl+X), the various file extensions used in the second folder is .exe, .jpg, .pdf, .mov, .rar, and .word, the diversity of file extensions is the same as in the first folder, the different is just size files and different hash result of SHA-1 value.

3. Results and Discussions

Based on the case simulation described above, two methods of removing evidence will be carried out in this study, namely the cut process (CTRL+X) and the delete process (Delete).

3.1 Identification

In this step, the evidence is identified to be used as a reference in the search for digital evidence based on the case that occurred. The evidence used is a Sandisk brand SDHC with specifications presented in Table 5.

Table 5. Specification SDHC

Spesifikasi	Type
Manufacture	SanDisk
Product	SanDisk Ultra
Series Memory	SDHC
Size Memory	32 GB
Speed Class	10
Ultra High Class	1
Max Speed	80 MB/s
Format	NTFS
IMEI	BM1815751525Z

3.2 Preservation

The evidence must be isolated to maintain its integrity at the preservation stage. A process is needed to ensure the evidence is still in its original state and has not changed logically. The action that needs to be taken is to move the side panel from normal (writeable) to a lock condition on SDHC. This causes the memory to change the mode to read-only, as shown in Figure 5.

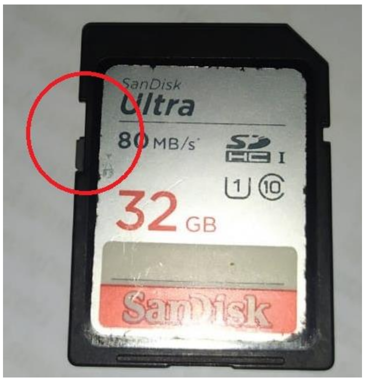
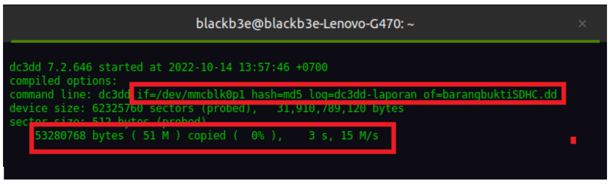


Figure 5. SDHC on Lock Condition

In read-only conditions, all data contained in the SDHC cannot be added, deleted or changed. This action is taken so that the forensic imaging collection process does not make changes when mirroring the SDHC.

3.3 Collection

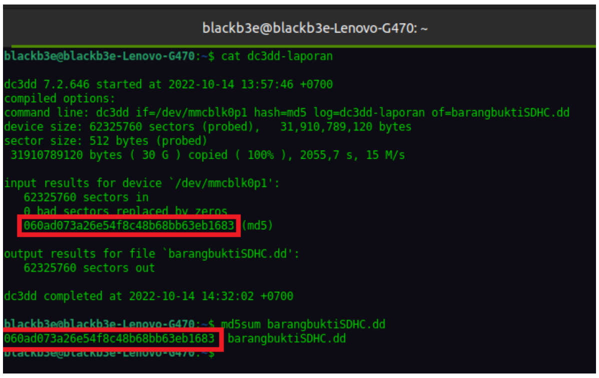
The third step is the examination and collection of digital evidence. Investigators are required to perform physical imaging or backup methods of evidence. This process is also known as acquisition. The acquisition tool used in this study is DC3DD, which can run on Linux operating systems. The output file after making the acquisition is in .dd format, in Figure 5 shows that the DC3DD process is making acquisitions, In this case DC3DD performs imaging at a speed of 15 Megabits per second, by activating the hash-on-fly feature using the md5 algorithm and generate file log namely “dc3dd laporan”.



```
dc3dd 7.2.646 started at 2022-10-14 13:57:46 +0700
compiled options:
command line: dc3dd if=/dev/mmcblk0p1 hash=md5 log=dc3dd-laporan of=barangbuktiSDHC.dd
device size: 62325760 sectors (probed),   31,910,789,120 bytes
sector size: 512 bytes (probed)
    53280768 bytes ( 51 M ) copied (  0% ),    3 s, 15 M/s
```

Figure 6. DC3DD Acquisition Process

After successfully carrying out the acquisition process, DC3DD will make a report on the results of the acquisition of evidence. To prove the evidence is original/valid, we must match the media hash and the results of the image acquisition carried out with DC3DD. As shown in Figure 7, the hash generated by the DC3DD acquisition process is the same as the hash generated by md5sum command on the digital evidence by linux terminal. It proves that the imaging validation of the evidence is valid. Based on figure 7 the start time for DC3DD to carry out imaging is 13:57 and it will end at 14:32, based on that DC3DD can completed the image acquisition with 35 minute and 16 second for size 31,910,789,120 bytes.



```
blackb3e@blackb3e-Lenovo-G470:~$ cat dc3dd-laporan

dc3dd 7.2.646 started at 2022-10-14 13:57:46 +0700
compiled options:
command line: dc3dd if=/dev/mmcblk0p1 hash=md5 log=dc3dd-laporan of=barangbuktiSDHC.dd
device size: 62325760 sectors (probed),   31,910,789,120 bytes
sector size: 512 bytes (probed)
 31910789120 bytes ( 30 G ) copied ( 100% ), 2055,7 s, 15 M/s

input results for device `/dev/mmcblk0p1':
   62325760 sectors in
   0 bad sectors replaced by zeros
   060ad073a26e54f8c48b68bb63eb1683 (md5)

output results for file `barangbuktiSDHC.dd':
   62325760 sectors out

dc3dd completed at 2022-10-14 14:32:02 +0700

blackb3e@blackb3e-Lenovo-G470:~$ md5sum barangbuktiSDHC.dd
060ad073a26e54f8c48b68bb63eb1683  barangbuktiSDHC.dd
blackb3e@blackb3e-Lenovo-G470:~$
```

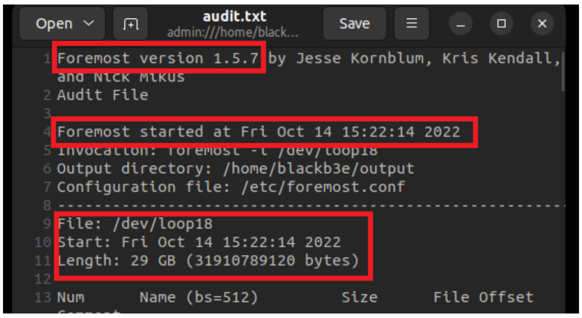
Figure 7. Hash Validation

3.4 Examination

In the data carving process, a search for files or data deleted and moved from the SDHC has been planned in the case simulation. In this step, a copy of the image that has been validated will then be searched using the foremost software tools. This process is called data carving. For every data carving process performed by foremost, there will be a report summary file that reads

DOI: https://doi.org/10.29207/resti.v6i6.4615

"audit.txt", The report on the results of the foremost process of data carving is presented in Figure 8, the report shows the version used when carving, namely foremost 1.5.7, in Figure 8, foremost starts doing data carving at 15:22:14, in Figure 9, it can be seen that the finishing time for foremost at 15:36:19, based on this, foremost takes 14 minutes and 5 seconds with a large image file of 29 Gigabytes.



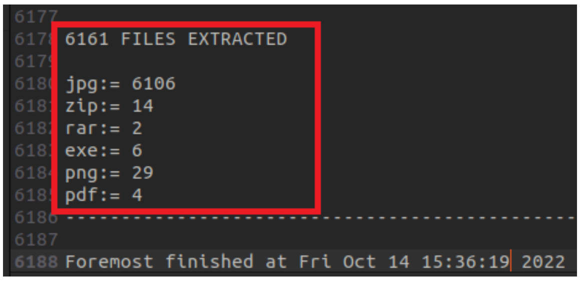
```
Foremost version 1.5.7 by Jesse Kornblum, Kris Kendall,
and Nick Mikus
Audit File

Foremost started at Fri Oct 14 15:22:14 2022
Invocation: foremost -i /dev/loop18
Output directory: /home/blackb3e/output
Configuration file: /etc/foremost.conf
------------------------------------------------------------------
File: /dev/loop18
Start: Fri Oct 14 15:22:14 2022
Length: 29 GB (31910789120 bytes)

Num      Name (bs=512)          Size       File Offset
```

Figure 8. Foremost Top Result

Figure 9 shows several file extensions that can be recovered by foremost, namely visual files with .jpg and .png extensions totaling 6135 files, compressed files with .rar and .zip extensions totaling 16 files, execution or application files totaling 6 files, and the last document file with .pdf extension is 4 files, the final report on foremost summary report informs the total files that were successfully recovered were 6161 files.



```
6161 FILES EXTRACTED

jpg:= 6106
zip:= 14
rar:= 2
exe:= 6
png:= 29
pdf:= 4
------------------------------------------------------------------

Foremost finished at Fri Oct 14 15:36:19 2022
```

Figure 9. Foremost Bottom Result

3.5 Analysis

In the analysis step, a hash value validation will be carried out for each file that can be successfully returned after carving data using foremost. Table 6 presents the results of string validation in groups of files that have gone through the delete process, there are 8 files that can be recovered by foremost, but 3 of them do not have the same hash value as the original file, then the file is declared invalid or has been manipulated, the remaining 7 files cannot be found.

Table 7 presents the results of string validation for groups of files that have gone through the transfer process (Ctrl+X), there are 9 files that can be recovered by foremost, but 5 of them do not have the same hash value as the original file, then the file is declared invalid or has been manipulated, the remaining 6 files cannot be found.

Table 6. Validation Hash sha1 deleted File

File Name	Hash SHA-1
file exe (1)	Not Found (Null)
file exe (2)	Invalid
file exe (3)	Invalid
file gambar (1)	valid
file gambar (2)	valid
file gambar (3)	valid
file pdf (1)	Not Found (Null)
file pdf (2)	Invalid
file pdf (3)	valid
filevideo (1)	Not Found (Null)
filevideo (2)	Not Found (Null)
filevideo (3)	Not Found (Null)
file winrar (1)	Not Found (Null)
file winrar (2)	valid
file winrar (3)	Not Found (Null)
file word (1)	valid
file word (2)	valid
file word (3)	valid

Table 7. Validation Hash sha1 Cut File

File Name	Hash SHA-1
file exe (4)	Not Found (Null)
file exe (5)	Invalid
file exe (6)	Invalid
file gambar (4)	Invalid
file gambar (5)	Invalid
file gambar (6)	Invalid
file pdf (4)	Valid
file pdf (5)	Not Found (Null)
file pdf (6)	Not Found (Null)
filevideo (4)	Not Found (Null)
filevideo (5)	Not Found (Null)
filevideo (6)	Not Found (Null)
file winrar (4)	Valid
file winrar (5)	Valid
file winrar (6)	Valid
file word (4)	Valid
file word (5)	Valid
file word (6)	Valid

3.6 Presentation

Based on the results obtained when the summary validation is presented in Table 8, in the extraction of the evidence image file as many as 30 files with different extensions, there are 23 files detected by foremost, in the files that can be detected, files with the .exe extension are the files with the smallest number of files to be recovered by foremost, and files with the .JPG extension are the files with the largest number of files to be recovered by foremost.

Table 8. Validation Result Summary

Extensi-ons file	Delete			Ctrl+X		
	Valid	invalid	Null	Valid	invalid	Null
*.exe	0	2	1	0	2	1
*.JPG	3	0	0	0	3	0
*.PDF	1	1	1	1	0	2
*.MOV	0	0	3	0	0	3
*.rar	1	0	2	3	0	0
*.docx	3	0	0	3	0	0
Total	8	3	7	7	5	6

DOI: https://doi.org/10.29207/resti.v6i6.4615

4. Conclusion

Based on the research conducted, the results can be obtained, several files can be returned at the examination stage using foremost by 77%, but only 50% of files have a valid hash string. There is a difference in the number of successful recoveries in the delete and transfer processes (Ctrl+X), the percentage of files that are deleted can be restored by foremost with a 73% chance of success, and on file transfers (Ctrl+x) the chance of success in recovery is 80%, the number of valid files after going through the file deletion process (delete) is 53%, and the number of valid files after going through the transfer process (Ctrl+X) is 47%. Therefore, it can be concluded that the results of DC3DD and Foremost processing in this study can be used as valid evidence.

References

[1] Mahkamah Agung, “Direktori Putusan Mahkamah Agung 2021-2022,” *Direktori Putusan*, 2022. https://putusan3.mahkamahagung.go.id/search.html?q=sdhc&jenis_doc=&cat=&jd=&tp=&court=&t_put=&t_upl=&t_pr=&t_reg=2021 (accessed Sep. 19, 2022).

[2] Mahkamah Agung, *Tindak Pidana Korupsi*. 2021. Accessed: Sep. 19, 2022. [Online]. Available: https://putusan3.mahkamahagung.go.id/direktori/putusan/zaec79e93c35dda085af313930353138.html

[3] A. Amirsoleimani *et al.*, “In-Memory Vector-Matrix Multiplication in Monolithic Complementary Metal–Oxide–Semiconductor-Memristor Integrated Circuits: Design Choices, Challenges, and Perspectives,” *Adv. Intell. Syst.*, vol. 2, no. 11, p. 2000115, Nov. 2020, doi: 10.1002/aisy.202000115.

[4] D. Quick and K.-K. R. Choo, “Pervasive social networking forensics: Intelligence and evidence from mobile device extracts,” *Spec. Issue Pervasive Soc. Netw.*, vol. 86, pp. 24–33, May 2017, doi: 10.1016/j.jnca.2016.11.018.

[5] P. Ruiz-de-Clavijo, E. Ostúa, M.-J. Bellido, J. Juan, J. Viejo, and D. Guerrero, “Minimalistic SDHC-SPI hardware reader module for boot loader applications,” *Microelectron. J.*, vol. 67, pp. 32–37, Sep. 2017, doi: 10.1016/j.mejo.2017.07.007.

[6] G. H. A. Kusuma and I. N. Prawiranegara, “Analisa Digital Forensik Rekaman Video CCTV dengan Menggunakan Metadata dan Hash,” *Vol .*, no. 1, p. 5, 2019.

[7] D. J. Hartono, “The Criminal Responsibility for Pornography Video Maker Through Digital Forensics on Social Media,” vol. 1, p. 8, 2022.

[8] G. Fanani, I. Riadi, and A. Yudhana, “Analisis Forensik Aplikasi Michat Menggunakan Metode Digital Forensics Research Workshop,” vol. 6, p. 9, 2022, doi: http://dx.doi.org/10.30865/mib.v6i2.3946.

[9] F. Anggraini and A. Yudhana, “Analisis Forensik Aplikasi TikTok Pada Smartphone Android Menggunakan Framework Association of Chief Police Officers,” vol. 9, no. 4, p. 11, 2022, doi: http://dx.doi.org/10.30865/jurikom.v9i4.4738.

[10] I. Riadi, R. Umar, and I. M. Nasrulloh, “Analisis Forensik Digital Pada Frozen Solid State Drive Dengan Metode National Institute Of Justice (NIJ),” *Elinvo Electron. Inform. Vocat. Educ.*, vol. 3, no. 1, pp. 70–82, Jul. 2018, doi: 10.21831/elinvo.v3i1.19308.

[11] A. Yudhana, I. Riadi, and I. Anshori, “Analisis Bukti Digital Facebook Messenger Menggunakan Metode Nist,” *IT J. Res. Dev.*, vol. 3, no. 1, pp. 13–21, Aug. 2018, doi: 10.25299/itjrd.2018.vol3(1).1658.

[12] R. Dinnur Rahman, I. Riadi, and The Society of Digital Information and Wireless Communication, “Framework Analysis of IDFIF V2 in WhatsApp InvestigationProcess on Android Smartphones,” *Int. J. Cyber-Secur. Digit. Forensics*, vol. 8, no. 3, pp. 213–222, 2019, doi: 10.17781/P002610.

[13] G. Horsman, “Formalising investigative decision making in digital forensics: Proposing the Digital Evidence Reporting and Decision Support (DERDS) framework,” *Digit. Investig.*, vol. 28, pp. 146–151, Mar. 2019, doi: 10.1016/j.diin.2019.01.007.

[14] B. Nikkel, “Fintech forensics: Criminal investigation and digital evidence in financial technologies,” *Forensic Sci. Int. Digit. Investig.*, vol. 33, p. 200908, Jun. 2020, doi: 10.1016/j.fsidi.2020.200908.

[15] P. Reedy, “Interpol review of digital evidence 2016 - 2019,” *Forensic Sci. Int. Synergy*, vol. 2, pp. 489–520, Jan. 2020, doi: 10.1016/j.fsisyn.2020.01.015.

[16] Imam Riadi, Abdul Fadlil, and Muhammad Immawan Aulia, “Investigasi Bukti Digital Optical Drive Menggunakan Metode National Institute of Standard and Technology (NIST),” *J. RESTI Rekayasa Sist. Dan Teknol. Inf.*, vol. 4, no. 5, pp. 820–828, Oct. 2020, doi: 10.29207/resti.v4i5.2224.

[17] I. Riadi, A. Fadlil, and M. I. Aulia, “Review Proses Forensik Optical Drive Menggunakan Metode National Institute of Justice (NIJ),” vol. 8, no. 3, p. 12, doi: http://dx.doi.org/10.35889/jutisi.v8i3.384.

[18] V. Ivanova, A. Boneva, Y. Doshev, S. Ivanov, and P. Vasilev, “Multifunctional Operating Station Based on Tcl/Tk and Its Applications,” in *2019 Big Data, Knowledge and Control Systems Engineering (BdKCSE)*, Nov. 2019, pp. 1–7. doi: 10.1109/BdKCSE48644.2019.9010662.

[19] E. Haryanto and I. Riadi, “Forensik Internet Of Things pada Device Level berbasis Embedded System,” *J. Teknol. Inf. Dan Ilmu Komput.*, vol. 6, no. 6, p. 703, Dec. 2019, doi: 10.25126/jtiik.2019661828.

[20] Nurhayati and N. Fikri, “The analysis of file carving process using PhotoRec and Foremost,” in *2017 4th International Conference on Computer Applications and Information Processing Technology (CAIPT)*, Kuta Bali, Aug. 2017, pp. 1–6. doi: 10.1109/CAIPT.2017.8320663.

[21] Ghoshal, S., Bandyopadhyay, P., Roy, S., & Baneree, M., “A journey from md5 to sha-3,” *Trends Commun. Cloud Big Data*, pp. 107–112, 2020.

[22] S. U. Lubis, “Implementasi Metode Md5 Untuk Mendeteksi Orisinalitas File Audio,” *KOMIK Konf. Nas. Teknol. Inf. Dan Komput.*, vol. 3, no. 1, Nov. 2019, doi: 10.30865/komik.v3i1.1620.

[23] D. Chang, M. Ghosh, S. K. Sanadhya, M. Singh, and D. R. White, “FbHash: A New Similarity Hashing Scheme for Digital Forensics,” *Digit. Investig.*, vol. 29, pp. S113–S123, Jul. 2019, doi: 10.1016/j.diin.2019.04.006.

[24] Stevens, M., Bursztein, E., Karpman, P., Albertini, A., & Markov, Y., “The first collision for full SHA-1,” *Annu. Int. Cryptol. Conf. Cham*, pp. 570–596, Aug. 2017.

[25] M. F. Hasa, A. Yudhana, and A. Fadlil, “Analisis Bukti Digital pada Storage Secure Digital Card Menggunakan Metode Static Forensic,” *Mob. Forensics*, vol. 1, no. 2, pp. 76–84, Nov. 2019, doi: 10.12928/mf.v1i2.1217.

[26] R. Montasari, “A standardised data acquisition process model for digital forensic investigations,” *Int J Inf. Comput. Secur.*, vol. 9, no. 3, p. 21, 2017.

[27] A. Powell and C. Haynes, “Social Media Data in Digital Forensics Investigations,” in *Digital Forensic Education: An Experiential Learning Approach*, X. Zhang and K.-K. R. Choo, Eds. Cham: Springer International Publishing, 2020, pp. 281–303. doi: 10.1007/978-3-030-23547-5_14.

[28] D. Mualfah and R. A. Ramadhan, “Analisis Forensik Metadata Kamera CCTV Sebagai Alat Bukti Digital,” *Digit. Zone J. Teknol. Inf. Dan Komun.*, vol. 11, no. 2, pp. 257–267, Nov. 2020, doi: 10.31849/digitalzone.v11i2.5174.

[29] I. Yaqoob, I. A. T. Hashem, A. Ahmed, S. M. A. Kazmi, and C. S. Hong, “Internet of things forensics: Recent advances, taxonomy, requirements, and open challenges,” *Future Gener. Comput. Syst.*, vol. 92, pp. 265–275, Mar. 2019, doi: 10.1016/j.future.2018.09.058.

[30] I. Riadi and P. Widiandana, “Cyberbullying Detection On Instant Messaging Services Using Rocchio And Digital Forensics Research Workshop Framework,” vol. 17, p. 15, 2022.

[31] A. Dimitriadis, N. Ivezic, B. Kulvatunyou, and I. Mavridis, “D4I - Digital forensics framework for reviewing and investigating cyber attacks,” *Array*, vol. 5, p. 100015, Mar. 2020, doi: 10.1016/j.array.2019.100015.