Infotekmesin
Vol.14, No.02, Juli 2023
p-ISSN: 2087-1627, e-ISSN: 2685-9858
DOI: 10.35970/infotekmesin.v14i2.1844, pp. 214-220

Comparative Analysis of Cloning-Hashing Applications for Securing Digital Evidence

Muhammad Nur Faiz*
Program Studi Rekayasa Keamanan Siber, Jurusan Teknik Informatika, Politeknik Negeri Cilacap
Jln. Dr. Soetomo No.1 Karangcengis Sidakaya, Kabupaten Cilacap, 53212, Indonesia
E-mail: faiz@pnc.ac.id

Info Naskah:
Naskah masuk: 31 Maret 2023
Direvisi: 14 Juni 2023
Diterima: 15 Juni 2023

Abstrak

Perkembangan Internet mengakibatkan variasi kejahatan siber meningkat. Kejahatan siber ini sangat erat kaitannya dengan bukti digital, sehingga penjahat siber cenderung menghapus, menyembunyikan, dan memformat semua data yang dikumpulkan untuk menghilangkan jejak bukti digital. Bukti digital ini sangat vital dalam pembuktian pada persidangan, maka diperlukan pengembangan aplikasi untuk mengamankan bukti digital. Penelitian ini bertujuan untuk membandingkan hasil kloning dan hashing dalam mengamankan bukti digital dan mengevaluasi kinerja aplikasi forensik digital yang dikembangkan dengan nama *Clon-Hash Application* v1 dibandingkan dengan aplikasi yang umumnya digunakan oleh penyidik antara lain Autopsy, FTK Imager, md5.exe dari segi fungsinya, hasilnya, penggunaan CPU. Hasil penelitian yang dilakukan bahwa proses kloning berhasil dengan sempurna dibuktikan dengan hasil nilai hash yang sama dengan aplikasi yang berbayar bahkan ada beberapa aplikasi lain yang belum dapat menampilkan nilai hash tersebut. Nilai hash pada aplikasi *Clon-Hash* v1 juga bervariasi dari MD5, SHA1 dan SHA256 yang belum ada pada aplikasi lain. Aplikasi yang dikembangkan lebih baik dari sisi fungsi, hasil dan penggunaan CPU.

Abstract

Keywords:
cloning;
hashing;
evidence;
security

The development of the Internet has resulted in an increasing variety of cyber crimes. Cybercrime is closely related to digital evidence, so cybercriminals tend to delete, hide, and format all collected data to eliminate traces of digital evidence. This digital evidence is very vital in proving at trial, so it is necessary to develop applications to secure digital evidence. This study aims to compare the results of cloning and hashing in securing digital evidence and evaluate the performance of a digital forensic application developed under the name Clon-Hash Application v1 compared to applications commonly used by investigators including Autopsy, FTK Imager, md5.exe in terms of its function, the result, CPU usage. The results of the research conducted show that the cloning process is perfectly successful, as evidenced by the hash value results which are the same as paid applications and there are even several other applications that have not been able to display the hash value. Hash values in the Clon-Hash v1 application also vary from MD5, SHA1, and SHA256 which do not exist in other applications. Applications developed are better in terms of function, results, and CPU usage.

***Penulis korespondensi:**
Muhammad Nur Faiz
E-mail: faiz@pnc.ac.id

1. Introduction

Society trends regarding technology have adopted many changes in the last few decades [1]. People often use different digital media like PCs, PDAs, laptops, cell phones, and some other digital devices and use them for communication purposes. One of the main sources of communication is the internet, the internet itself can cause several crimes or better known as cybercrimes, which result in damage such as data theft or dangerous system activities [2]. The people who have the responsibility to commit such cybercrimes are required for their capabilities and procedures to prevent or carry out such attacks [3]. These cybercriminals have discovered and found innovative and innovative ways to commit crimes using today's advanced technology [4]. In addition, perpetrators have also created new crimes such as identity theft, cyberstalking, and ransomware [5]. These violations are labeled as cybercrimes and explicitly with digital technology which makes many systems today vulnerable, and becomes a tool that supports criminal activities considering that the tools and methods are easy to find on the Internet [6].

According to the [7] in Indonesia from January 1, 2022, to September 17, 2022, the crime in figure 1 Most of the threats were 2,354 reports. Meanwhile, the second most common crime received by cyber patrols was gambling, with 1,872 cases. Crimes in the form of imprisonment as many as 841 cases and 659 cases of extortion. This makes the Directorate of Cyber Crimes at the Indonesian National Police must always evaluate the development of current crimes. Digital developments, apart from having a positive impact, also have a negative impact. The negative impact is the emergence of various crimes that are varied so criminal investigators must be good at tracking the history of using communication tools such as transactions, messages, and other forms of digital media based on demographics. location, individual address, bank account, passport, or another identifier, and more. Investigators (including law enforcement agencies) can trace electronic tracks through audit trails and punish perpetrators based on digital evidence. Even though the electronic evidence is thoroughly examined by the criminal process, this makes investigators have to be careful because this digital evidence can be easily controlled [8].

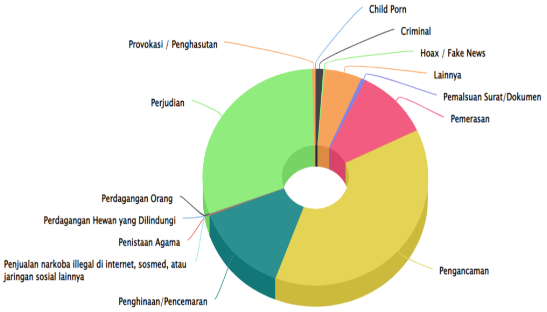


Figure 1. Police Reports made by the civil public Period 01 January 2022 to 17 September 2022 [7].

In the legal process, it is very important to critically evaluate the quality and authenticity of the evidence in order to avoid an unjustified decision. The accuracy of digital forensic science has always been a concern, and still is; it is under debate. The National Institute of Standards Technology (NIST) USA [9] as a reference institution for digital forensics investigations and digital evidence handling in the world strongly criticizes all traditional analytical techniques such as DNA matching, fingerprints, bite marks, and firearm marks, footprints, and more. They refuse to recognize it as an exact and exact science. In addition, it is emphasized to establish clear scientific standards to verify the validity and reliability of digital forensics methods and allow the use of only scientifically proven methods in court, advocating the use of best practices in digital forensics. Digital forensics methods, which do not have proper authentication and solid statistical basis to justify different reasons and results are unacceptable. In addition, methods that do not meet the standards of systematic, objectivity, and independence are also not approved in current legal practice [10].

This Digital Evidence faces difficulties in meeting the standards of scientific criteria in court [11]. The lack of trust in digital forensics processes and the absence of a set set of rules for evaluation provide a smooth and accessible avenue for defense attorneys to challenge the evidence in courtrooms [12]. They found several loopholes in the process of collecting and comparing evidence to create reasonable doubts over the accuracy and credibility of the evidence [13]. Some cases also dispute the validity of digital forensics applications and methods. In digital forensics investigations, the authenticity and integrity of the evidence referred to as digital evidence is very important so it encourages the need to give critical attention to the process or procedure used in obtaining the evidence [6]. This study aims to explore applications in digital evidence maintenance such as cloning and hashing. Analyze the results of cloning and hashing of several relevant applications to scientifically validate the security of digital evidence.

Digital evidence has been recognized in accordance with the Law of the Republic of Indonesia Number 19 of 2016 concerning Electronic Information and Transactions, that electronic information and/or electronic documents and/or their printed results are legal evidence [14]. Digital evidence can be found on computer hard disks, cell phones, iPods, pen drives, digital cameras, CDs, DVDs, diskettes, computer networks, the Internet, and more [15]. Digital evidence that can be used as evidence, such as URL addresses that have been visited, e-mail messages or a collection of registered email addresses, word processing programs or extension formats used, spreadsheet documents used, image formats used if found, deleted or formatted files, passwords, windows registry, hidden files, event viewers logs, and application logs, including checking metadata [16]. Digital evidence can also be linked to online banking fraud, online stock trading fraud, source code theft, credit card fraud, tax evasion, virus attacks, cyber sabotage, phishing attacks, email hijacking, denial of service, hacking, murder cases, organized crime, operations terrorists, insults, pornography, extortion, smuggling.

According to the U.S. Department of Justice [17] [18] there are three things in obtaining digital evidence: a). Measures taken in securing and collecting digital evidence must not affect the integrity of the data; b). In testing digital evidence must be someone who has been trained; c). All activities related to the retrieval, testing, storage or transfer of digital evidence must be documented and subject to retesting.

According to J. Richter [19], there are five characteristics of digital evidence, namely: Admissible (Decent and acceptable), Authentic (Original), Complete (Complete), Reliable (Available) and Believable (Trusted). The explanation for each characteristic of digital evidence is as follows: a). Admissible, Digital evidence must be in accordance with the facts and problems that occur. The evidence submitted must also be accepted and used for the sake of law, starting from research interests to court x; b). Authentic (Original), Evidence must have a clear legal relationship with the case being investigated and evidence is not the result of engineering. Digital evidence must be proven in court that the evidence is original and has never been altered; c). Complete, The evidence must be complete and be able to prove the evil acts committed by the perpetrators of the crime. The evidence collected is not enough just based on one perspective of an event that took place. The information that has been collected, for example, is in the form of a trace entering a system, so the data collected is not only the log data of the perpetrator of the crime, but all the logs that enter the system, because it could actually be that before the perpetrator committed a crime, there were other people who helped him and/or there who committed the crime before the first perpetrator; d). Reliable The evidence collected must be available and reliable. This evidence must be able to be used as evidence in court and the process of collecting evidence and analysis carried out must be in accordance with procedures; e). Believable (Trusted) Evidence and presentations made in court must be understandable by judges and trustworthy. It is useless to present evidence in court such as about binary if the judge does not understand it. The process of submitting evidence in court must use lay language that can be understood by judges.

Several studies regarding the handling of digital evidence, research [20] implements the concept of inventory data, namely the concept of management of physical evidence through control of physical evidence and all activities related to physical evidence can be maintained and can be well documented. This research focuses on data storage that still uses a DBMS so that the physical evidence stored is still visible. Further development is focused on the security of stored data using either encryption or other methods. An integrated system is needed between physical evidence and digital evidence storage systems. Subsequent research on digital evidence, namely research on the application of multi smart contracts, explains that digital evidence has different characteristics and different information details between one type of digital evidence, images, audio, video, and documents or other types of digital evidence. The addition of more detailed information on digital evidence with Multi Smart Contracts can improve the integrity and accuracy of digital evidence and can help simplify and speed up investigators or experts in determining actions in examining managed digital evidence. This research [21] builds middleware by connecting naive chains to multi smart contracts using an API in the form of URLs that are accessed using the curl function on multi smart contracts.

Further research, regarding the flexibility of a repository based on SAN (Storage Area Network) and web-based technology is used as a network-based centralized storage architecture. This system is expected to help law enforcement agencies in terms of traceability management for digital evidence. Subsequent research on digital evidence, namely research that results in developing a proposed digital evidence management system can improve the accessibility of digital evidence which is very influential in the investigation process. Starting from the stage of submitting digital evidence, downloading digital evidence of storage to downloading the chain of custody form, it is done online without having to come to the digital forensic laboratory so that the investigation process runs faster and minimizes the risk of damage to digital evidence and the safety of officers. This research also focuses on dealing with COVID-19 because it can be accessed online by officers. Although there are many studies related to the handling of digital evidence, there is currently no specific research on the development of applications for digital evidence maintenance for cloning and hashing processes. Based on these reasons, this research was carried out with the aim of developing applications for digital evidence maintenance, especially the cloning and hashing processes, because generally investigators only use pre-existing applications.

2. Method

2.1 Methodology

Digital forensics research methods in this study adopted digital forensics methods from the National Institute of Standards Technology (NIST). Digital forensics method is used to describe the stages of forensics that will be carried out, can find out the flow of research in a structured manner and can be a reference in solving existing problems. The digital forensic steps can be seen in Figure 2.

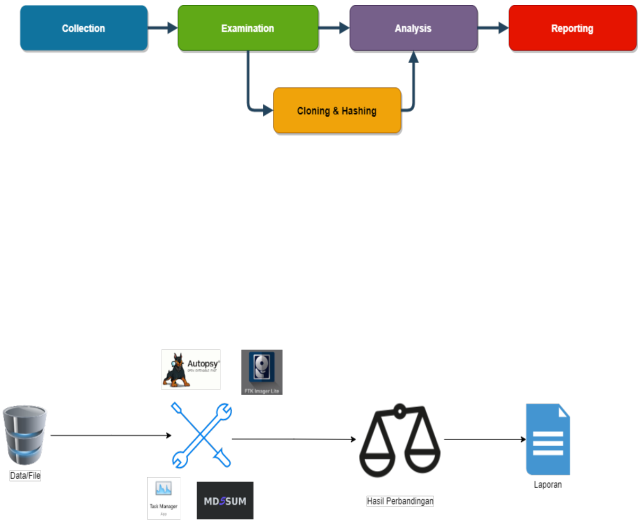


Figure 2. Digital Forensic Investigation of the National Institute of Standards Technology (NIST) [22]

Based on Figure 2, the digital forensic process defined by the National Institute of Standards and Technology (NIST) consists of the following phases:

1) Collection, the purpose of which is to identify potential sources of data relevant to events and then label and record them. After that, the data located at the source must be obtained while maintaining the integrity of the source.
2) Examination, which involves assessing the data obtained from the Data collection and extracting the Phase relevant to the incident while maintaining its integrity. In this inspection phase, there are two processes, namely cloning and hashing. This cloning is to duplicate the digital evidence according to the original, then the hashing process itself to validate the digital evidence and whether it really matches the original or not.
3) Analysis, which involves studying the information extracted by examination to answer the 5WH question or determine that no or partial conclusions can be drawn.
4) Reporting, namely the process of preparing and presenting procedures, methods, and tools used in the investigation along with the results of the analysis phase.

2.2 Case Scenario

This research requires a scenario to get validation about the cloning-hashing application by comparing existing applications. Applications used such as FTK Imager, Autopsy, md5sum, and developed applications. The scenario stages include collecting data from different file types, then the data is duplicated which is then carried out by hashing, the application used for testing up to CPU usage or resources on the device used. Basically in digital forensics artifacts from the use of applications can also potentially damage evidence.

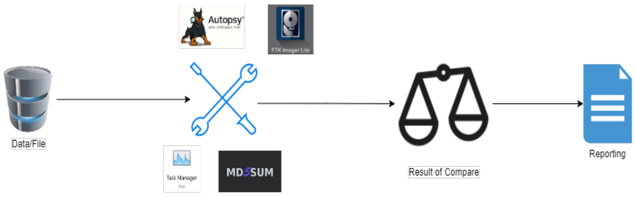


Figure 3. Cloning-hashing Testing Scenario

Table 1. Files and Applications

File	Capacity	Application
Mem	18,325,504 KB	• FTK Imager 4.5.0.3
dd	15,360 KB	• Autopsy 4.7.0
JPG	32 KB	• md5sum.exe
Mp4	6366 KB	• Clon-Hash v1 Apllication
PDF	301 KB	
Doc	111 KB	
PPT	2651	
exe	48 KB	

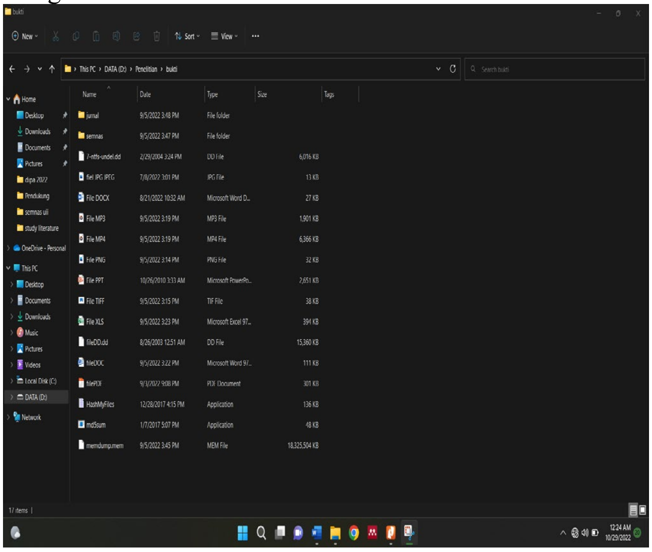
The test scenario is shown in Figure 3. An explanation of the files tested with several applications used in this study is shown in table 1. Applications are tested and compared with the results of cloning and hashing along with resource usage.

3. Result and Discussion

The result of this research is to compare analysis performance of digital forensics applications in cloning, hashing, and resource performance in maintaining digital evidence using the National Institute of Standards Technology (NIST) framework.

3.1 Collection Phase

At the stage of collecting the target files are files with different extensions and different capacities as well. There is a capacity of 18 GB which may contain potential evidence. In this file collection stage later all files will be tested from the cloning results and hash values, scenarios including through cloning and hashing results from Autopsy, FTK Imager, and Clon-Hash v1 Applications. After collecting the next step is to maintain and examine the digital evidence. 8 files with different capacities and extensions are also shown in figure 4.

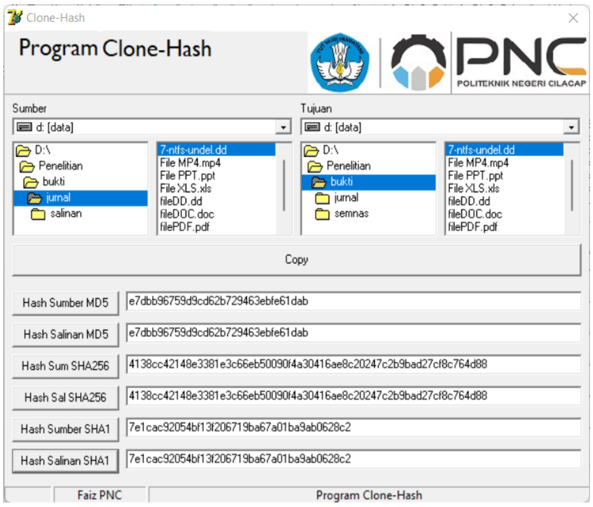


Name	Date	Type	Size	Tags
jurnal	9/5/2022 3:48 PM	File folder		
semnas	9/5/2022 3:47 PM	File folder		
7-ntfs-undel.dd	2/29/2004 3:24 PM	DD File	6,016 KB	
fiel JPG JPEG	7/8/2022 3:01 PM	JPG File	13 KB	
File DOCX	8/21/2022 10:32 AM	Microsoft Word D...	27 KB	
File MP3	9/5/2022 3:19 PM	MP3 File	1,901 KB	
File MP4	9/5/2022 3:19 PM	MP4 File	6,366 KB	
File PNG	9/5/2022 3:14 PM	PNG File	32 KB	
File PPT	10/26/2010 3:33 AM	Microsoft PowerPo...	2,651 KB	
File TIFF	9/5/2022 3:15 PM	TIF File	38 KB	
File XLS	9/5/2022 3:23 PM	Microsoft Excel 97...	394 KB	
fileDD.dd	8/26/2003 12:51 AM	DD File	15,360 KB	
fileDOC	9/5/2022 3:22 PM	Microsoft Word 97...	111 KB	
filePDF	9/3/2022 9:08 PM	PDF Document	301 KB	
HashMyFiles	12/28/2017 4:15 PM	Application	136 KB	
md5sum	1/7/2017 5:07 PM	Application	48 KB	
memdump.mem	9/5/2022 3:45 PM	MEM File	18,325,504 KB	

Figure 4. Digital File Evidence to be tested

3.2 Examination Phase

The Testing Phase is the stage where digital evidence is tested from the evidence that has been collected in the original file in accordance with what was obtained at the crime scene (TKP). This stage is a validation process by securing digital evidence by cloning the original evidence and comparing the cloned results with the hash value because for the integrity of the file or file it must be authentic according to the original. The application developed to maintain digital evidence is shown in figure 5.



Clone-Hash

Program Clone-Hash

Sumber: d: [data]

Tujuan: d: [data]

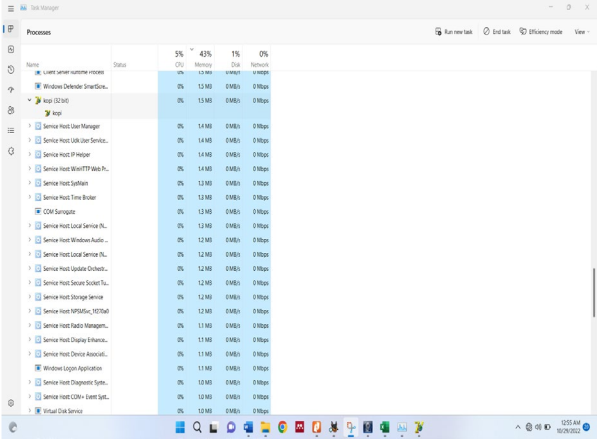
Sumber folder	Sumber file	Tujuan folder	Tujuan file
D:\	7-ntfs-undel.dd	D:\	7-ntfs-undel.dd
Penelitian	File MP4.mp4	Penelitian	File MP4.mp4
bukti	File PPT.ppt	bukti	File PPT.ppt
jurnal	File XLS.xls	jurnal	File XLS.xls
salinan	fileDD.dd	semnas	fileDD.dd
	fileDOC.doc		fileDOC.doc
	filePDF.pdf		filePDF.pdf

Hash Sumber MD5	e7dbb96759d9cd62b729463ebfe61dab
Hash Salinan MD5	e7dbb96759d9cd62b729463ebfe61dab
Hash Sum SHA256	4138cc42148e3381e3c66eb50090f4a30416ae8c20247c2b9bad27cf8c764d88
Hash Sal SHA256	4138cc42148e3381e3c66eb50090f4a30416ae8c20247c2b9bad27cf8c764d88
Hash Sumber SHA1	7e1cac92054bf13f206719ba67a01ba9ab0628c2
Hash Salinan SHA1	7e1cac92054bf13f206719ba67a01ba9ab0628c2

Faiz PNC | Program Clone-Hash

Figure 5. A Cloning and hashing process in the Clon-Hash v1 Application

Figure 5 shows the results of cloning and hashing of the 7-ntfs-undel.dd file, the source file from the "journal" folder to the destination "proof" folder with the hash value of MD5 the same, SHA256 and SHA1 showing the same results. MD5 hash value "e7dbb96759d9cd62b729463ebfe61dab". The next series tests the performance of the resource when running the Clone-Hash v1 application, which only recently running there is no cloning and hash process because the cloning and hash process should not leave artifacts that can eliminate potential evidence. This is shown in Figure 6.



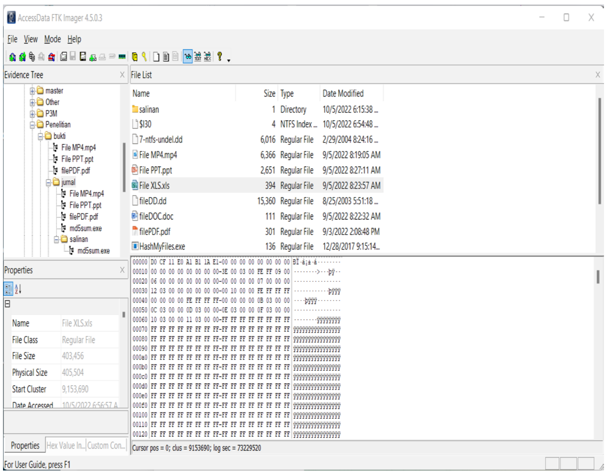
Task Manager

Processes

Name	Status	5% CPU	43% Memory	1% Disk	0% Network
Client Server Runtime Process		0%	1.5 MB	0 MB/s	0 Mbps
Windows Defender SmartScre...		0%	1.5 MB	0 MB/s	0 Mbps
kopi (32 bit)		0%	1.5 MB	0 MB/s	0 Mbps
kopi					
Service Host: User Manager		0%	1.4 MB	0 MB/s	0 Mbps
Service Host: Udk User Service...		0%	1.4 MB	0 MB/s	0 Mbps
Service Host: IP Helper		0%	1.4 MB	0 MB/s	0 Mbps
Service Host: WinHTTP Web Pr...		0%	1.4 MB	0 MB/s	0 Mbps
Service Host: SysMain		0%	1.3 MB	0 MB/s	0 Mbps
Service Host: Time Broker		0%	1.3 MB	0 MB/s	0 Mbps
COM Surrogate		0%	1.3 MB	0 MB/s	0 Mbps
Service Host: Local Service (N...		0%	1.3 MB	0 MB/s	0 Mbps
Service Host: Windows Audio ...		0%	1.2 MB	0 MB/s	0 Mbps
Service Host: Local Service (N...		0%	1.2 MB	0 MB/s	0 Mbps
Service Host: Update Orchestr...		0%	1.2 MB	0 MB/s	0 Mbps
Service Host: Secure Socket Tu...		0%	1.2 MB	0 MB/s	0 Mbps
Service Host: Storage Service		0%	1.2 MB	0 MB/s	0 Mbps
Service Host: NPSMSvc_1f270a0		0%	1.2 MB	0 MB/s	0 Mbps
Service Host: Radio Managem...		0%	1.1 MB	0 MB/s	0 Mbps
Service Host: Display Enhance...		0%	1.1 MB	0 MB/s	0 Mbps
Service Host: Device Associati...		0%	1.1 MB	0 MB/s	0 Mbps
Windows Logon Application		0%	1.1 MB	0 MB/s	0 Mbps
Service Host: Diagnostic Syste...		0%	1.0 MB	0 MB/s	0 Mbps
Service Host: COM+ Event Syst...		0%	1.0 MB	0 MB/s	0 Mbps
Virtual Disk Service		0%	1.0 MB	0 MB/s	0 Mbps

Figure 6. Resource usage when running Clon-Hash v1 application

Figure 6 shows that when the application is run it is still low and small. This proves that the application is not too burdensome for the performance of device resources. Seen only 1.5MB for memory and CPU 0%. The next process compares with other applications such as FTK Imager.



AccessData FTK Imager 4.5.0.3

File List

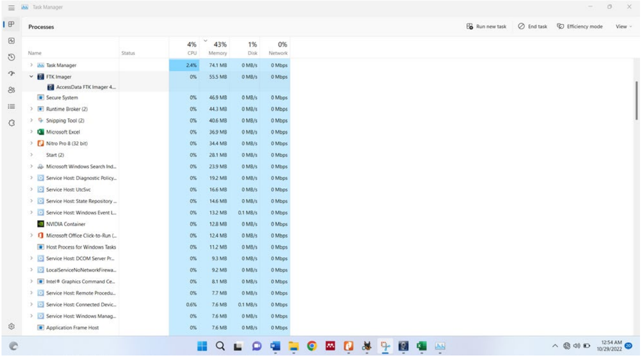
Name	Size	Type	Date Modified
salinan	1	Directory	10/5/2022 6:15:38 ...
$I30	4	NTFS Index ...	10/5/2022 6:54:48 ...
7-ntfs-undel.dd	6,016	Regular File	2/29/2004 8:24:16 ...
File MP4.mp4	6,366	Regular File	9/5/2022 8:19:05 AM
File PPT.ppt	2,651	Regular File	9/5/2022 8:27:11 AM
File XLS.xls	394	Regular File	9/5/2022 8:23:57 AM
fileDD.dd	15,360	Regular File	8/25/2003 5:51:18 ...
fileDOC.doc	111	Regular File	9/5/2022 8:22:32 AM
filePDF.pdf	301	Regular File	9/3/2022 2:08:48 PM
HashMyFiles.exe	136	Regular File	12/28/2017 9:15:14...

Name	File XLS.xls
File Class	Regular File
File Size	403,456
Physical Size	405,504
Start Cluster	9,153,690
Date Accessed	10/5/2022 6:56:57 A...

```
00000 D0 CF 11 E0 A1 B1 1A E1-00 00 00 00 00 00 00 00 ÐÏ·à¡±·á········
00010 00 00 00 00 00 00 00 00-3E 00 03 00 FE FF 09 00 ········>···þÿ··
00020 06 00 00 00 00 00 00 00-00 00 00 00 07 00 00 00 ················
00030 12 03 00 00 00 00 00 00-00 10 00 00 FE FF FF FF ············þÿÿÿ
00040 00 00 00 00 FE FF FF FF-00 00 00 00 0B 03 00 00 ····þÿÿÿ········
00050 0C 03 00 00 0D 03 00 00-0E 03 00 00 0F 03 00 00 ················
00060 10 03 00 00 11 03 00 00-FF FF FF FF FF FF FF FF ········ÿÿÿÿÿÿÿÿ
00070 FF FF FF FF FF FF FF FF-FF FF FF FF FF FF FF FF ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
00080 FF FF FF FF FF FF FF FF-FF FF FF FF FF FF FF FF ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
00090 FF FF FF FF FF FF FF FF-FF FF FF FF FF FF FF FF ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
000a0 FF FF FF FF FF FF FF FF-FF FF FF FF FF FF FF FF ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
000b0 FF FF FF FF FF FF FF FF-FF FF FF FF FF FF FF FF ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
000c0 FF FF FF FF FF FF FF FF-FF FF FF FF FF FF FF FF ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
000d0 FF FF FF FF FF FF FF FF-FF FF FF FF FF FF FF FF ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
000e0 FF FF FF FF FF FF FF FF-FF FF FF FF FF FF FF FF ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
000f0 FF FF FF FF FF FF FF FF-FF FF FF FF FF FF FF FF ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
00100 FF FF FF FF FF FF FF FF-FF FF FF FF FF FF FF FF ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
00110 FF FF FF FF FF FF FF FF-FF FF FF FF FF FF FF FF ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
00120 FF FF FF FF FF FF FF FF-FF FF FF FF FF FF FF FF ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
```

Cursor pos = 0; clus = 9153690; log sec = 73229520

Figure 7. A cloning and hashing process in the FTK Imager application



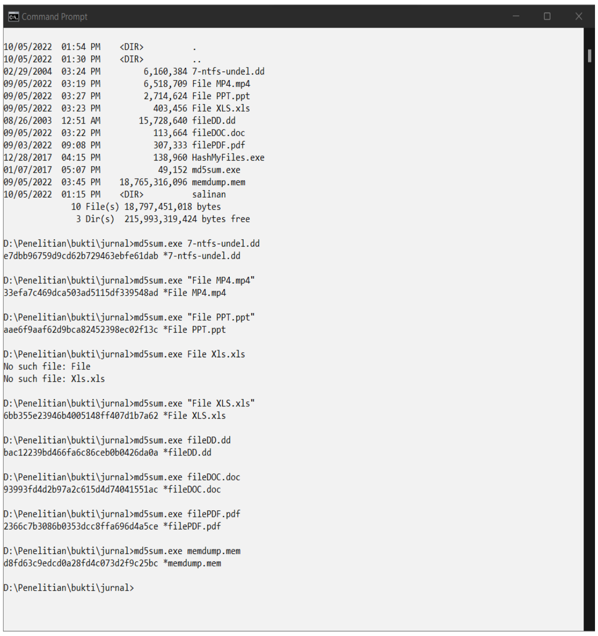
Task Manager

Processes

Name	Status	4% CPU	43% Memory	1% Disk	0% Network
Task Manager		2.4%	74.1 MB	0 MB/s	0 Mbps
FTK Imager		0%	55.5 MB	0 MB/s	0 Mbps
AccessData FTK Imager 4...					
Secure System		0%	46.9 MB	0 MB/s	0 Mbps
Runtime Broker (2)		0%	44.3 MB	0 MB/s	0 Mbps
Snipping Tool (2)		0%	40.6 MB	0 MB/s	0 Mbps
Microsoft Excel		0%	36.9 MB	0 MB/s	0 Mbps
Nitro Pro 8 (32 bit)		0%	34.4 MB	0 MB/s	0 Mbps
Start (2)		0%	28.1 MB	0 MB/s	0 Mbps
Microsoft Windows Search Ind...		0%	23.9 MB	0 MB/s	0 Mbps
Service Host: Diagnostic Policy...		0%	19.2 MB	0 MB/s	0 Mbps
Service Host: UtcSvc		0%	16.6 MB	0 MB/s	0 Mbps
Service Host: State Repository ...		0%	14.6 MB	0 MB/s	0 Mbps
Service Host: Windows Event L...		0%	13.2 MB	0.1 MB/s	0 Mbps
NVIDIA Container		0%	12.8 MB	0 MB/s	0 Mbps
Microsoft Office Click-to-Run (...		0%	12.4 MB	0 MB/s	0 Mbps
Host Process for Windows Tasks		0%	11.2 MB	0 MB/s	0 Mbps
Service Host: DCOM Server Pr...		0%	9.3 MB	0 MB/s	0 Mbps
LocalServiceNoNetworkFirewa...		0%	9.2 MB	0 MB/s	0 Mbps
Intel® Graphics Command Ce...		0%	8.1 MB	0 MB/s	0 Mbps
Service Host: Remote Procedu...		0%	7.7 MB	0 MB/s	0 Mbps
Service Host: Connected Devic...		0.6%	7.6 MB	0.1 MB/s	0 Mbps
Service Host: Windows Manag...		0%	7.6 MB	0 MB/s	0 Mbps
Application Frame Host		0%	7.6 MB	0 MB/s	0 Mbps

Figure 8. Resource usage when running FTK Imager application

Figure 7 shows FTK Imager during the cloning and hashing process, the hash process on FTK Imager itself must export the hash value and requires another application to open the result of the hash value. The hash value after being exported and opened with another application, the MD5 hash value of the 7-ntfs-undel.dd file, is "e7dbb96759d9cd62b729463ebfe61dab". Figure 8 shows that when the FTK Imager application used memory capacity is 55.5 MB, and the CPU usage is 0%. This proves that the application takes up quite a lot of memory resources, this does not rule out the possibility of having an impact on digital evidence that has the potential to become primary evidence. The next process is to run the Autopsy Application. Autopsy application uses 1,179.4 MB memory capacity, and 0% CPU usage. This proves that the application takes up quite a lot of memory resources, even up to 1GB, this does not rule out the possibility of having an impact on digital evidence that has the potential to become primary evidence.



```
10/05/2022  01:54 PM    <DIR>          .
10/05/2022  01:30 PM    <DIR>          ..
02/29/2004  03:24 PM         6,160,384 7-ntfs-undel.dd
09/05/2022  03:19 PM         6,518,709 File MP4.mp4
09/05/2022  03:27 PM         2,714,624 File PPT.ppt
09/05/2022  03:23 PM           403,456 File XLS.xls
08/26/2003  12:51 AM        15,728,640 fileDD.dd
09/05/2022  03:22 PM           113,664 fileDOC.doc
09/03/2022  09:08 PM           307,333 filePDF.pdf
12/28/2017  04:15 PM           138,960 HashMyFiles.exe
01/07/2017  05:07 PM            49,152 md5sum.exe
09/05/2022  03:45 PM    18,765,316,096 memdump.mem
10/05/2022  01:15 PM    <DIR>          salinan
              10 File(s) 18,797,451,018 bytes
               3 Dir(s)  215,993,319,424 bytes free

D:\Penelitian\bukti\jurnal>md5sum.exe 7-ntfs-undel.dd
e7dbb96759d9cd62b729463ebfe61dab *7-ntfs-undel.dd

D:\Penelitian\bukti\jurnal>md5sum.exe "File MP4.mp4"
33efa7c469dca503ad5115df339548ad *File MP4.mp4

D:\Penelitian\bukti\jurnal>md5sum.exe "File PPT.ppt"
aae6f9aaf62d9bca82452398ec02f13c *File PPT.ppt

D:\Penelitian\bukti\jurnal>md5sum.exe File Xls.xls
No such file: File
No such file: Xls.xls

D:\Penelitian\bukti\jurnal>md5sum.exe "File XLS.xls"
6bb355e23946b4005148ff407d1b7a62 *File XLS.xls

D:\Penelitian\bukti\jurnal>md5sum.exe fileDD.dd
bac12239bd466fa6c86ceb0b0426da0a *fileDD.dd

D:\Penelitian\bukti\jurnal>md5sum.exe fileDOC.doc
93993fd4d2b97a2c615d4d74041551ac *fileDOC.doc

D:\Penelitian\bukti\jurnal>md5sum.exe filePDF.pdf
2366c7b3086b0353dcc8ffa696d4a5ce *filePDF.pdf

D:\Penelitian\bukti\jurnal>md5sum.exe memdump.mem
d8fd63c9edcd0a28fd4c073d2f9c25bc *memdump.mem

D:\Penelitian\bukti\jurnal>
```

Figure 9. the Results of hash values md5 application

Figure 9 shows that the Autopsy application cannot read the hash value of the 7-ntfs-undel.dd file, so this application is not good for securing digital evidence. md5.exe application that runs on a windows terminal. This md5 application is classified as very little in taking resources including memory and CPU because it runs on the operating system terminal (cmd). This proves that the application is not too burdensome for the performance of device resources. The MD5 hash value of the 7-ntfs-undel.dd file is “e7dbb96759d9cd62b729463ebfe61dab”.

3.3 Result of Comparison

Figure 9 shows that the Autopsy application cannot read the hash value of the 7-ntfs-undel.dd file, so this application is not good for securing digital evidence. md5.exe application that runs on a windows terminal. This md5 application is classified as very little in taking

Table 2. Cloning Test Comparison Results on Applications

Eks	Cloning			
	Clon-Hash	FTK Imager	Autopsy	md5
Mem	√	√	√	X
dd	√	√	√	X
JPG	√	√	√	X
Mp4	√	√	√	X
PDF	√	√	√	X
Doc	√	√	√	X
PPT	√	√	√	X
exe	√	√	√	X

Table 3. Hashing Test Comparison Results on Applications

Eks	Hashing			
	Clon-Hash	FTK Imager	Autopsy	md5
Mem	√	√	X	√
dd	√	√	X	√
JPG	√	√	X	√
Mp4	√	√	X	√
PDF	√	√	X	√
Doc	√	√	X	√
PPT	√	√	X	√
exe	√	√	X	√

4. Conclusion

This study concludes that the application developed under the name Clon-Hash v1 is successful. When compared with Autopsy, FTK Imager, this application uses less CPU resources. The Clon-Hash v1 application is better in terms of user interface because it makes it easier for users to operate when compared to md5.exe. The cloning test was successfully proven with the exact same hash value between the original file and the cloned file. Hash values also vary from MD5, SHA1, and SHA256 which do not yet exist in other applications, because the digital forensics standard is the MD5 hash. Application development research for the cloning process and further development has been carried out, with file type extensions, capacities, encryption passwords, and adding application comparators such as forensic toolkits, belkasoft, oxygen and others.

Acknowledgement

This research can be carried out with the help of funds from the Daftar Isian Pelaksanaan Anggaran (DIPA) Politeknik Negeri Cilacap.

References

[1] R. J. Alzahrani and A. Alzahrani, “Security analysis of ddos attacks using machine learning algorithms in networks traffic,” *Electron.*, vol. 10, no. 23, 2021, doi: 10.3390/electronics10232919.

[2] M. N. Faiz and W. A. Prabowo, “Comparison of Acquisition Software for Digital Forensics Purposes,” *Kinet. Game Technol. Inf. Syst. Comput. Network, Comput. Electron. Control*, vol. 4, no. 1, pp. 37–44, Nov. 2018, doi: 10.22219/kinetik.v4i1.687.

[3] I. Y. Anggraini, S. Sucipto, and R. Indriati, “Cyberbullying Detection Modelling at Twitter Social Networking,” *JUITA J. Inform.*, vol. 6, no. 2, p. 113, 2018, doi: 10.30595/juita.v6i2.3350.

[4] W. Y. Sulistyo, I. Riadi, and A. Yudhana, “Penerapan Teknik SURF pada Forensik Citra untuk Analisa Rekayasa Foto Digital,” *JUITA J. Inform.*, vol. 8, no. 2, p. 179, 2020, doi: 10.30595/juita.v8i2.6602.

[5] N. Al Mutawa, J. Bryce, V. N. L. Franqueira, and A. Marrington, “Forensic investigation of cyberstalking cases using Behavioural Evidence Analysis,” in *Digital Investigation*, 2016, vol. 16. doi: 10.1016/j.diin.2016.01.012.

[6] M. Riskiyadi, “Investigasi Forensik Terhadap Bukti Digital Dalam Mengungkap Cybercrime,” *Cyber Secur. dan Forensik Digit.*, vol. 3, no. 2, pp. 12–21, 2020, doi: 10.14421/csecurity.2020.3.2.2144.

[7] Direktorat Tindak Pidana Siber Bareskrim Polri, “Jumlah Laporan Polisi yang dibuat masyarakat,” *patrolisiber.id*, 2022. https://patrolisiber.id/

[8] A. Setya and A. Suganda, “Design of Digital Evidence Collection Framework in Social Media Using SNI 27037: 2014,” *JUITA J. Inform.*, vol. 10, no. 1, p. 127, 2022, doi: 10.30595/juita.v10i1.13149.

[9] R. Umar, A. Yudhana, and M. N. Faiz, “Experimental analysis of web browser sessions using live forensics method,” *Int. J. Electr. Comput. Eng.*, vol. 8, no. 5, 2018, doi:

10.11591/ijece.v8i5.pp.2951-2958.

[10] A. F. Moussa, “Electronic evidence and its authenticity in forensic evidence,” *Egypt. J. Forensic Sci.*, vol. 11, no. 1, p. 20, Dec. 2021, doi: 10.1186/s41935-021-00234-6.

[11] R. Murray, “MemTri: A Memory Forensics Triage Tool using Bayesian Network and Volatility,” University of Westminster, 2016. [Online]. Available: https://www.researchgate.net/profile/Rohan_Murray/publication/308340060_MemTri_A_Memory_Forensics_Triage_Tool_using_Bayesian_Network_and_Volatility/links/57e1577108aecd35d4a06cf0.pdf

[12] H. Arshad, A. Jantan, G. Keng, and A. Sahar, “A multilayered semantic framework for integrated forensic acquisition on social media,” *Digit. Investig.*, vol. 29, pp. 147–158, 2019, doi: 10.1016/j.diin.2019.04.002.

[13] W. Pranoto, I. Riadi, and Y. Prayudi, “Perbandingan Tools Forensics pada Fitur TRIM SSD NVMe Menggunakan Metode Live Forensics,” *It J. Res. Dev.*, vol. 4, no. 2, pp. 135–148, 2020, doi: 10.25299/itjrd.2020.vol4(2).4615.

[14] Republik Indonesia, *Undang-Undang Republik Indonesia Nomor 19 Tahun 2016 Tentang Informasi Dan Transaksi Elektronik*, no. 1. 2016, pp. 1–31. [Online]. Available: https://web.kominfo.go.id/sites/default/files/users/4761/UU 19 Tahun 2016.pdf

[15] M. N. Faiz, W. A. Prabowo, and M. F. Sidiq, “Studi Komparasi Investigasi Digital Forensik pada Tindak Kriminal,” *Journal of Informatics, Information System, Software Engineering and Applications (INISTA)*, vol. 1, no. 1. pp. 63–70, 2018. doi: 10.20895/INISTA.V1I1.

[16] M. F. Sidiq and M. N. Faiz, “Review Tools Web Browser Forensics untuk Mendukung Pencarian Bukti Digital,” *J. Edukasi dan Penelit. Inform.*, vol. 5, no. 1, pp. 67–73, 2019, doi: 10.26418/jp.v5i1.31430.

[17] A. Ajijola, P. Zavarsky, and R. Ruhl, “A review and comparative evaluation of forensics guidelines of NIST SP 800-101 Rev.1:2014 and ISO/IEC 27037:2012,” in *2014 World Congress on Internet Security, WorldCIS 2014*, 2014, pp. 66–73. doi: 10.1109/WorldCIS.2014.7028169.

[18] U.S. Department of Justice Office of Justice Programs, “Electronic Crime Scene Investigation: A Guide for First Responders, Second Edition,” 2001. [Online]. Available: http://www.iwar.org.uk/ecoespionage/resources/cybercrime/ecrime-scene-investigation.pdf

[19] J. Richter, N. Kuntze, and C. Rudolph, “Securing digital evidence,” in *5th International Workshop on Systematic Approaches to Digital Forensic Engineering, SADFE 2010*, 2010, pp. 119–130. doi: 10.1109/SADFE.2010.31.

[20] M. B. Pakarti, D. H. Fudholi, and Y. Prayudi, “Manajemen Pengelolaan Bukti Digital Untuk Meningkatkan Aksesibilitas Pada Masa Pandemi Covid-19,” *J. Ilm. SINUS*, vol. 19, no. 1, p. 27, 2021, doi: 10.30646/sinus.v19i1.502.

[21] A. S. Putra and Y. Prayudi, “Implementasi Multi Smart Contract pada Bukti Digital dan Chain of Custody dalam Meningkatkan Keamanan dan Integritas Bukti Digital,” *JUSTINDO (Jurnal Sist. dan Teknol. Inf. Indones.*, vol. 6, no. 2, pp. 98–108, 2021, doi: 10.32528/justindo.v6i2.3945.

[22] R. Umar, A. Yudhana, and M. Nur Faiz, “Experimental Analysis of Web Browser Sessions Using Live Forensics Method,” *Int. J. Electr. Comput. Eng.*, vol. 8, no. 5, p. 2951, 2018, doi: 10.11591/ijece.v8i5.pp2951-2958.