Data Recovery Comparative Analysis using Open-based Forensic Tools Source on Linux

Muhammad Fahmi Abdillah[1]
Department of Informatics
The Islamic University of Indonesia
Yogyakarta, Indonesia

Yudi Prayudi[2]
Department of Informatics
The Islamic University of Indonesia
Yogyakarta, Indonesia

***Abstract*—Data recovery is one of the forensic techniques used to recover data that has been lost or deleted. Data recovery is carried out if there is a condition where the data that has been owned is deleted or damaged. If the data has been lost or deleted or even tampered with, then a forensic expert has several ways to restore data that has been lost or damaged. One of them is to use a complete data recovery method using forensic tools, namely, TSK Recover, FTK Imager, Foremost Recover, and Testdisk Recover. Unfortunately, tools such as FTK imager and TSK recover have a weakness, namely that some damaged or corrupted data files cannot be restored in their entirety; they can only be recovered but not be opened. This study uses a tool comparison method approach using foremost recover and Testdisk recover. It's just that this method cannot be used using the graphic user interface (GUI) but using the CLI (Command Line) in the LINUX operating system. And the files that have been recovered will be fully recovered.**

***Keywords*—Recovery; tools; FTK imager; foremost; Testdisk**

I. INTRODUCTION

Data loss is a condition where the data that has been owned becomes corrupted or deleted [1]. According to several researchers, there are many companies or individuals who accidentally delete their personal data. It is very important for digital forensic analysts to have the right tools to recover data [2]. All devices store a lot of important data and information that is always used for personal and corporate purposes. Forensic tools are used by thousands of digital forensic professionals. The functionality of forensic tools varies greatly [3].

Currently, there are many simple data recovery tools; several features have been provided consistently for more effective forensic extraction to get the whole data [4]. including image storage, file data hashing, data visualization, and data carving on damaged images. However, most of these tools are paid for [5]. Due to the limited inspection features, the extracted data cannot be ported directly to the circuit to extract additional evidence. In this study, I present several tools that will help forensic analysts perform open source-based data recovery on Linux [6].

Data recovery is the process of recovering a problematic or lost system so that it can be recovered as usual [7]. Data recovery is also a forensic technique that is often used to search for digital artifacts that have been lost or deleted from devices such as cellphones, computers, and laptops [8]. Data backup, which is a preventive measure that is intentionally done to protect data by copying or copying data to other storage media [9].

This study aims to determine the forensic tools that are useful today and in the future. To overcome the occurrence of data loss, a digital forensics expert is needed [10]. Data recovery is one of the techniques that must be mastered by digital forensic experts [11]. If there is data damage or data loss, then it is the job of a forensics officer to recover data that has been lost or damaged [12]. Several cases of data corruption or data loss are one of the challenges that digital forensics experts must face. There are several data recovery tools used by digital forensic experts, such as Autopsy, FTK imager, TSK recover, Foremost, and Testdisk [13].

In the case of previous research, many forensic experts use this tool as a tool to find evidence [14]. This tool is very helpful for recovering data that has been lost or damaged, but this tool has a certain weakness, when restoring data or data recovery, namely data that has been damaged can only be recovered but cannot be opened in its entirety, therefore the solution what is needed is a complete recovery, data that has been retrieved / damaged can be recovered and reopened the same as before. To overcome this problem, a forensic expert uses recovery tools in a storage [15].

Recovery of the data to be recovered is in the allocated space and unallocated space [16]. This space stores all files that are still available and can be read logically, and stores all files that are no longer available, even if they have been deleted from storage and cannot be read logically [17].

From some of the references found, it can be concluded that previous research related to the themes discussed included many case studies that used forensic tools and used several methods to recover lost data [18]. The data is stored in various storage devices such as flash drives, HDDs, SSDs, and RAM. The storage is on mobile devices, computers, and even servers. Data recovery methods also vary depending on the storage to be processed. One of them is using autopsy tools or other forensic tools [19]. This tool is very helpful for forensic experts to find lost data files, such as JPG, MP4, PDF, PNG, Doc, Zip, Rar files, and so on. It's just that this tool has certain weaknesses when it comes to data retrieval or data recovery. Data that has been damaged can only be recovered but cannot be opened in its entirety. Therefore, the solution needed is full

recovery. Data that has been lost or damaged can be recovered and reopened the same as before [20].

Efforts to provide data recovery solutions for handling digital evidence on a storage device such as a smartphone have been discussed by Wilson & Chi (2017) using digital forensic tools to make it easier to acquire data. The most important thing about recovering data is the recovery method because there are many ways to acquire and recover data [12].

However, there are several researchers who provide reviews of data recovery with different techniques and different devices, as discussed by Povar & Bhadran (2011). The carving technique is what is meant. This technique helps in finding hidden or deleted files from digital media or with the data acquisition technique that has been discussed by Jo et al. (2016) regarding data acquisition using forensic tools, namely Autopsy. This technique is very helpful for a forensic expert to collect data or evidence [21].

Several films and photographs in the form of corrupted or damaged JPG, MP4 and PNG files will be used as part of the data to help solve this issue. Additionally, it will be processed afterwards using a number of forensic programs, including Testdisk Recover, Foremost, and the Sleuth Kit Autopsy. These tools will receive this data and begin the recovery procedure [22]. The final step allows for a comparison of numerous efficient tools that can be used to carry out a complete recovery. Using digital forensic tools to aid data capture, Wilson & Chi outline efforts to provide data recovery solutions for digital evidence on a storage device like a smartphone. Since there are numerous ways to obtain and recover data, the recovery method is the most crucial factor [23]. Using a live forensics procedure with the Formost recovery program or Testdisk recover is the suggested solution for flawless data recovery. Data can be acquired with this tool from storage devices as HDD, SSD, FD, CD/DVD, zip, and rar [12].

This study compares the forensic tool settings that will be utilized to recover deleted or damaged data in the form of data file formats that will be used as evidence in cybercrime case resolution [24]. In this investigation, data recovery is carried out on Linux utilizing the live forensic method. The findings of this study should aid in our understanding of digital forensics, particularly with regard to data recovery [18].

A forensic technique applied while the system is operating is called live forensics. This is because when the system is switched off, the data that needs to be recovered can be lost. This live forensic technique is typically applied to memory scenarios where data can be written to or erased from—this type of memory is also known as volatile memory or non-volatile memory [25].

II. Research Method

The procedures needed to conduct a study are known as the research technique. These procedures are taken so that a scientific process can be used to tackle the difficulties that develop by providing logical and systematic solutions, as shown in Fig. 1.

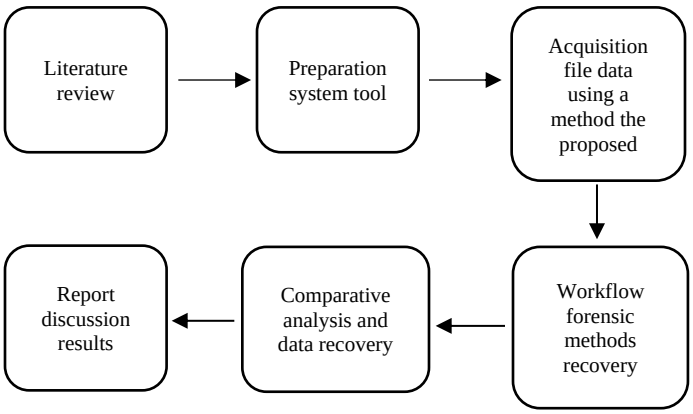

Fig. 1. Research Methodology.

A. A Study of the Literature

In order to support the overall objective of this research, the purpose of this literature review is to gather information materials on research topics that can be sourced from articles, papers, journals, papers in the form of theories, research reports, or previous findings. We also visit several websites on the internet that is related to these theories about digital forensics, evidence, and recovery.

B. Tools for System Preparation

This is a step in creating the hardware and software specifications needed for research projects like planning and putting into practice a comparative examination of data recovery utilizing a flash drive. Such as setting up the system and installing software. The physical machine has Microsoft Windows 11 Home installed as its operating system. The employment of physical computer hardware and software as research tools and materials is necessary for the successful operation of the experimental implementation. The following tools and materials are employed in this process:

- MSI Modern 14 laptop with specifications:
  a. Processor : Intel Core ™ I7-10510U CPU 1.80Ghz
  b. Memory : 512 GB / 8 GB RAM
  c. OS : Windows 11 home insider 64-bit
- Flashdisk 8 GB
- TSK recover tool
- Foremost recover tool
- Testdisk Recover tool
- Oracle VM virtual box (CSI Linux)

C. Proposed Methodology

1) Foremost Recover Forensic Method

In order to replicate the functionality of the DOS carving software for usage on the Linux platform, the most recent recovery technique was developed in March 2001. Special agents Kris Kendall and Jesse Kornblum from the Office of Special Investigations of the US Air Force originally wrote

Formost. The program was altered in 2005 as part of a master's thesis by Nick Mikus, a researcher at the Naval Graduate School's Center for Information Security Studies and Research. Among these changes were improved accuracy and foremost extraction rates.

This method is intended to read and copy data straight from the disk into the computer's memory without taking into account the underlying file system type. The method of file carving is used by Formost Recover to look for header file types that coincide with those in the formost configuration file. There are no alternatives for a graphical user interface, hence the command line interface is primarily used. The JPG, GIF, PNG, BMP, AVI, EXE, MPG, WAV, RIFF, WMV, MOV, PDF, PLE, DOC, ZIP, RAR, HTM, and CPP file formats can all be recovered using the first approach. Additional file types can be specified in the configuration file formost.conf, which is typically located in /usr/local/etc. It can be used to recover data from hard disks that use the ex3, NTFS, or FAT file systems as well as directly from picture files. In example, it can be used to retrieve data from a smartphone via a computer as shown in Fig. 2.

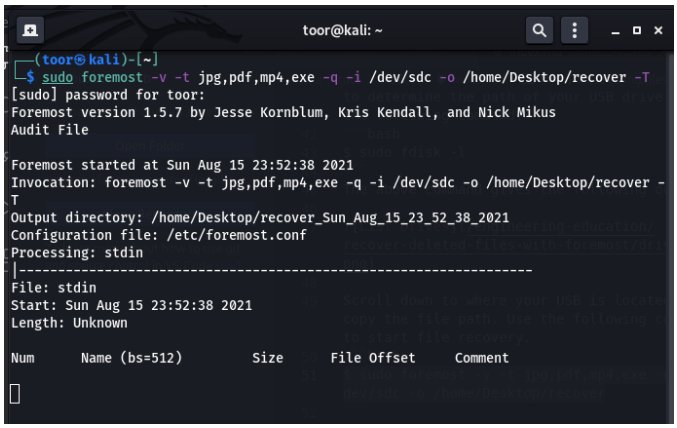

Fig. 2. Example Image Foremost Recover Method.

2) Testdisk Recover Forensic Method

A free and open-source utility called Testdisk is used to recover data from missing or deleted partitions. There is no user interface version of this utility; it is CLI driven. A digital forensics specialist can utilize this to restore partitions that are unable to boot due to things like virus attacks and, of course, purposeful or unintentional destruction of the partition table. This testdisk can also do a number of additional tasks, including:

- Recover FAT32 boot sector from backup
- Recover boot sector FAT12/FAT16/FAT32
- Recover NTFS boot sector
- Restore NTFS boot sector from backup
- Fix MFT using MFT mirror
- Find backup superblocks ext2/ext3/ext4
- Undelete file from FAT, exFAT, NTFS, and ext2 file system
- Copy file from FAT, exFAT, NTFS and partitions deleted ext2/ext3/ext4

A forensic expert who is looking into a case involving data loss or corruption will find this Testdisk to be of great assistance. Fig. 3 depicts a sample of the Testdisk recover technique.

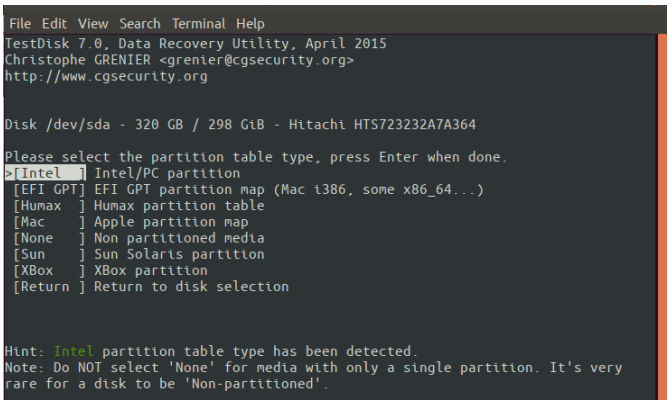

Fig. 3. Example Image Testdisk Recover Method.

D. Recovery Method Workflow

Workflow recovery methods are phases or steps that digital examiners must go through when performing digital tasks, beginning with preparation, extraction, and analysis. As shown in Fig. 4.

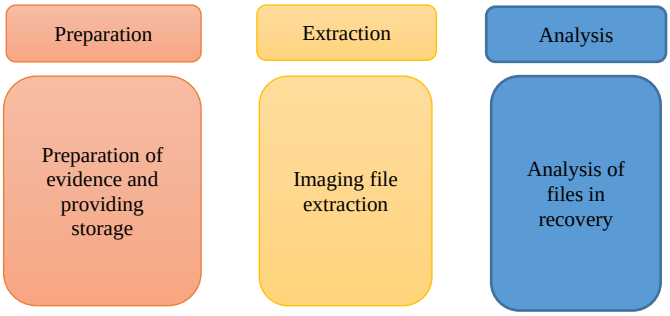

Fig. 4. Workflow Method Recovery.

- Preparation

By providing storage space for data that will be recovered and extracted, we set the stage.

- Extraction

This carries out file extraction by locating and restoring deleted files. The properties of the file structure, deleted data, file name, file size, and location will all be made known through file extraction.

- Analysis

It is in the process of analyzing the outcomes of file-checking. In order to assess or evaluate the success of data file extraction and can suggest the technologies that are best for file recovery in this investigation.

E. Data Recovery Comparative Analysis

Using forensic tools like TSK recover, Formost, and Testdisk recovery, the data recovery stage of comparative analysis was extracted. Damaged data files like JPG, PNG, and MP4 on flash drives, HDDs, SSDs, and other storage will be examined using a data file recovery approach utilizing a number of tools, which will then discover variations that impact data recovery on these tools so that they may be opened again. in full. Tables I and II show many tables that depict the outcomes of the recovery based on the findings of the forensic investigation.

TABLE I. FLASHDISK DATA RECOVERY RESULTS

Storage	Flasdisk	
Tools	TSK recover, FTK imager, Foremost, Testdisk	
Jenis File	JPG, PNG, MP4	
Recovery status	Succeed	Not successful
	√	

TABLE II. HDD/SSD DATA RECOVERY RESULTS

Storage	HHD / SSD	
Tools	TSK recover, FTK imager, Foremost, Testdisk	
Jenis File	JPG, PNG, MP4	
Recovery status	Succeed	Not successful
	√	

III. RESULTS AND DISCUSSIONS

A. Preparation

By providing storage space for the data that will be recovered and extracted, the preparation stage is prepared. In this study, we used flash storage that contained unopenable rar files containing JPG, PNG, and MP4 files. The tests and findings obtained have as their goal getting a full recovery file so you can compare the forensic tools utilized. Some of these files are hashed, as indicated in Tables III and IV, to demonstrate their validity in comparison to the findings of forensic analysis and recovery.

TABLE III. MD5 HASH

No	Data file	Initial MD5 Hash
1	.JPG	459d4d4d38993bb270d9f8d7d5029a5c
2	.PNG	120695b94e5d3bf867862eb42715a4a4
3	.MP4	677f7dca67cdf3741d3f924a668fc2b2

TABLE IV. SHA1 HASH

No	Data file	Initial SHA1 Hash
1	.JPG	1b036089c09444fe5ae1fb0f4279de1f99200fa8
2	.PNG	ccc7286c0ba4a4fb1a61a1793dfa4fc8b60ef60d
3	.MP4	13d1fcd6ef10140dc80726640564aabee08a6161

B. Extraction

File extraction will also expose the characteristics of the file structure, deleted data, file name, file stamps, file size, and location during the extraction stage, which is to extract files by locating and recovering deleted files. The tools that aid in the extraction process run on Linux and use Guysmager using the tools TestDisk and Foremost for data recovery.

Another independent acquisition tool that may be used to clone disks and make forensic pictures is Guymager. Guymager, created by Guy Voncken, is entirely open source, only works on Linux-based hosts, and shares many of the same capabilities as DCLDD. Guymager, the forensic imager included in this package, is made to operate quickly, support a variety of image file types, and be extremely user-friendly. It leverages parallel compression in its high-speed multi-threaded engine to maximize performance on multi-processor and hyper-threading engines. It is shown in Fig. 5.

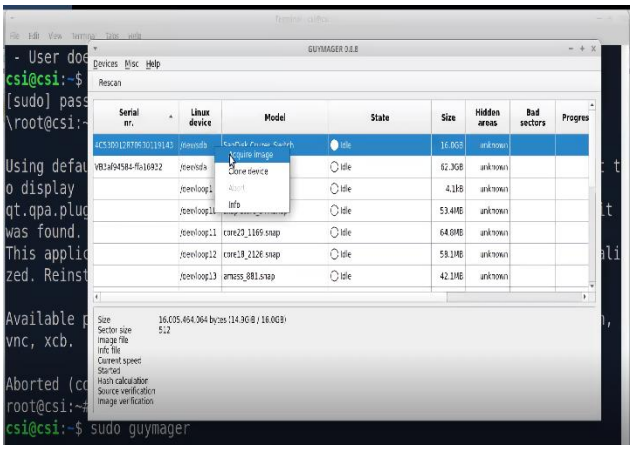

Fig. 5. The Process of Mounting File in Guymager.

1) Recovery Process

The recovery step involves a data recovery procedure using a number of programs for comparison, including TestDisk Recovery, TSK Recovery, FTK Imager, and Foremost. After that, the recovery process will use the extracted files. One of the Linux CLI-based tools for data recovery is the TSK recover utility. There are some JPG files that cannot be accessed, as illustrated in Fig. 6; however the recovery procedure utilizing the TSK recover tool was successfully recovered.

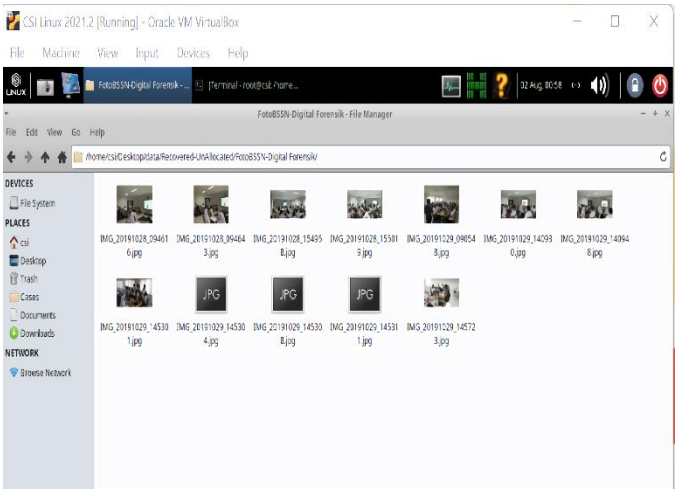

Fig. 6. File Recovery Process on TSK Recover.

A tool that is frequently used for imaging files is the FTK Imager. The FTK Imager has a number of features, including:

- Functions & Features
- Full Disk Forensic Image
- File Decryption & Password Crack
- Parsing Registry Files
- Collect, Process, and Analyze Data Sets Containing Apple's File System
- Locate, Manage and Filter Mobile Data
- Visualization Technology

This utility is frequently used to restore erased data. However, it is clear that allocated and unallocated files differ throughout the recovery step. As seen in Fig. 7, it is a file that can be recovered but cannot be opened.

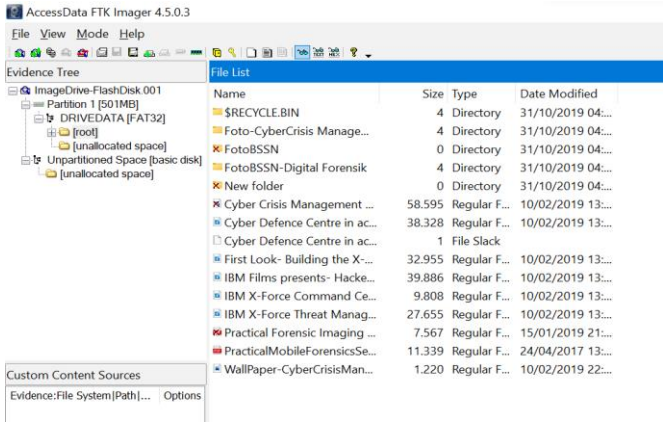

Fig. 7. File Recovery Process on FTK Imager.

The Foremost Recovery Tool is a program created to read and copy certain areas of the disk straight into the computer's memory while ignoring the underlying file system type. For the majority of recovers, it employs a technique called file carving to search for header file types that coincide with those contained in the primary configuration file. The best recovery tool for JPG files has been used to successfully recover all of the files. It is shown in Fig. 8.

```
Foremost started at Tue Jun 21 03:41:55 2022
Invocation: foremost -v -o foremost-JPG -t jpg -i /dev/loop3p1
Output directory: /home/csi/Desktop/data/foremost-JPG
Configuration file: /etc/foremost.conf
------------------------------------------------------------------
File: /dev/loop3p1
Start: Tue Jun 21 03:41:55 2022
Length: 501 MB (525336576 bytes)

Num      Name (bs=512)         Size      File Offset     Comment

0:      00008224.jpg          729 KB         4210688
1:      00009688.jpg          636 KB         4960256
2:      00010968.jpg          349 KB         5615616
3:      00011672.jpg          547 KB         5976064
4:      00012768.jpg          370 KB         6537216
5:      00013512.jpg          357 KB         6918144
6:      00014232.jpg          993 KB         7286784
7:      00016224.jpg         1016 KB         8306688
8:      00018264.jpg          788 KB         9351168
```

Fig. 8. File Recovery Process on Foremost Recover.

Data can be recovered from lost or deleted partitions using the free and open-source Testdisk recover utility. A digital forensics specialist can restore partitions that are unable to boot due to reasons including malware attacks and purposeful or unintentional loss of the partition table using this CLI-based application, which does not have a user interface version. Fig. 9 illustrates how the recovery procedure using the Testdisk recover program was successful in restoring lost and damaged files.

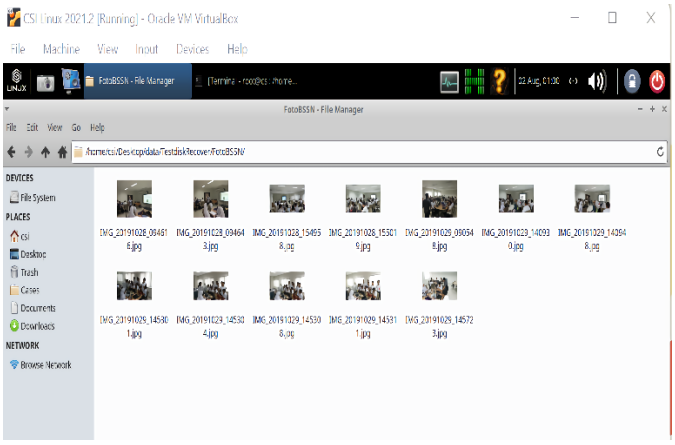

Fig. 9. File Recovery Process on Testdisk Recover.

C. Analysis

The analysis step is where the outcomes of the files that have been checked are examined. A comparison of the data recovery tools, when situations like missing or damaged files arise, you must use the resources at your disposal to find a solution. You must experiment with all of the forensic tools, not just one. It makes sense that certain tools are unable to recover files perfectly while others are successful in doing so, as in this study is shown by Tables V and VI.

TABLE V. RESULTS OF STATUS RECOVERY ALLOCATED FILES

No	Tools	Status File Recovery		
		JPG	PNG	MP4
		Allocated		
1	TSK Recover	100%	100%	100%
2	FTK Imager	100%	100%	100%
3	Foremost Recover	100%	100%	100%
4	TestDisk	100%	100%	100%

A sort of file storage known as allocated space is still accessible, and the files contained therein can still be read logically. All files in the designated space can be fully recovered after conducting research with the aforementioned instruments.

TABLE VI. RESULTS OF UNALLOCATED FILES RECOVERY STATUS

No	Tools	Status File Recovery		
		JPG	PNG	MP4
		UnAllocated		
1	TSK Recover	50%	50%	100%
2	FTK Imager	50%	50%	100%
3	Foremost Recover	100%	100%	100%
4	TestDisk	100%	100%	100%

Files that are no longer accessible or have been erased and cannot be read logically are stored in unallocated space. Not all files have been totally and flawlessly retrieved after utilizing the following utility to do research on data files in unallocated space

IV. CONCLUSION

Based on the results of research on the comparison of data recovery using open source-based tools on Linux, the results of the comparison of these tools with previous research are very different. Due to the limited features available in open source forensic tools like the TSK recover tool and FTK Imager; it makes investigators hard to get valid evidence. It can be concluded that among these tools there are those that can recover data files that have been damaged and can be reopened in their entirety and some are not. One of the open source based tools that can be used is foremost recover and Testdisk recover. This tool is a solution to the problem of recovery. Of the tools that have been tested, only 50% have been fully recovered. Namely, TSK recover and FTK imager. While the foremost tool, Testdisk, can recover 100% completely. However, tools that can't recover completely don't mean they're not good. These tools are still recommended and can be used to assist investigators in the investigation process. Investigators can have several options for forensic tools to carry out the investigative process. This study aims to determine the forensic tools that are useful today and in the future.

REFERENCES

[1] P. Dibb and M. Hammoudeh, “Forensic data recovery from android os devices: An open source toolkit,” Proc. - 2013 Eur. Intell. Secur. Informatics Conf. EISIC 2013, no. May, p. 226, 2013, doi: 10.1109/EISIC.2013.58.

[2] M. Breeuwsma and M. De Jongh, “Forensic data recovery from flash memory,” Small Scale Digit. …, vol. 1, no. 1, pp. 1–17, 2007, [Online]. Available: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.135.5697&rep=rep1&type=pdf%5Cnhttp://www.ssddfj.org/papers/SSDDFJ_V1_1_Breeuwsma_et_al.pdf

[3] Y. Guo and J. Slay, “Chapter 21 DATA RECOVERY FUNCTION TESTING,” Ifip Int. Fed. Inf. Process., pp. 297–311, 2010.

[4] J. Buchanan-Wollaston, T. Storer, and W. Glisson, “Comparison of the Data Recovery Function of Forensic Tools,” IFIP Adv. Inf. Commun. Technol., vol. 410, pp. 331–347, 2013, doi: 10.1007/978-3-642-41148-9_22.

[5] I. P. A. E. Pratama, “Computer Forensic Using Photorec for Secure Data Recovery Between Storage Media: a Proof of Concept,” Int. J. Sci. Technol. Manag., vol. 2, no. 4, pp. 1189–1196, 2021, doi: 10.46729/ijstm.v2i4.256.

[6] M. P. Mohite and S. B. Ardhapurkar, “Design and implementation of a cloud based computer forensic tool,” Proc. - 2015 5th Int. Conf. Commun. Syst. Netw. Technol. CSNT 2015, pp. 1005–1009, 2015, doi: 10.1109/CSNT.2015.180.

[7] J. Plum and A. Dewald, “Forensic APFS file recovery,” ACM Int. Conf. Proceeding Ser., 2018, doi: 10.1145/3230833.3232808.

[8] Y. Guo, J. Slay, and J. Beckett, “Validation and verification of computer forensic software tools-Searching Function,” Digit. Investig., vol. 6, no. SUPPL., pp. S12–S22, 2009, doi: 10.1016/j.diin.2009.06.015.

[9] J. N. Hilgert, M. Lambertz, and D. Plohmann, “Extending the Sleuth Kit and its underlying model for pooled storage file system forensic analysis,” DFRWS 2017 USA - Proc. 17th Annu. DFRWS USA, vol. 22, pp. S76–S85, 2017, doi: 10.1016/j.diin.2017.06.003.

[10] I. Riadi, S. Sunardi, and S. Sahiruddin, “Analisis Forensik Recovery pada Smartphone Android Menggunakan Metode National Institute Of Justice (NIJ),” J. Rekayasa Teknol. Inf., vol. 3, no. 1, p. 87, 2019, doi: 10.30872/jurti.v3i1.2292.

[11] M. S. Simanjuntak and J. Panjaitan, “Analisa Recovery Data Menggunakan Software,” J. Tek. Inform. Komput. Univers., vol. 1, no. 1, pp. 26–32, 2021.

[12] R. Wilson and H. Chi, “A case study for mobile device forensics tools,” Proc. SouthEast Conf. ACMSE 2017, pp. 154–157, 2017, doi: 10.1145/3077286.3077564.

[13] I. Zuhriyanto, A. Yudhana, and I. Riadi, “Analisis Perbandingan Tools Forensic pada Aplikasi Twitter Menggunakan Metode Digital Forensics Research Workshop,” J. Resti, vol. 1, no. 3, pp. 829–836, 2017.

[14] H. Handrizal, “Analisis Perbandingan Toolkit Puran File Recovery, Glary Undelete Dan Recuva Data Recovery Untuk Digital Forensik,” J-SAKTI (Jurnal Sains Komput. dan Inform., vol. 1, no. 1, p. 84, 2017, doi: 10.30645/j-sakti.v1i1.31.

[15] I. Riadi, Sunardi, and Sahiruddin, “Perbandingan Tool Forensik Data Recovery Berbasis Android Menggunakan Metode Nist,” J. Teknol. Inf. dan Ilmu Komput., vol. 7, no. 1, pp. 197–204, 2020, doi: 10.25126/jtiik.202071921.

[16] J. Panjaitan and A. C. Sitepu, “Analisis Kinerja Forensic Acquisition Tools Untuk,” vol. 1, no. 2, pp. 17–25, 2021.

[17] D. S. I. Krisnadi, “Citra Forensik Dari Barang Bukti Elektronik Dengan Metode Physical Menggunakan Acquisition Tools Tableau Imager Dan Ftk Imager,” p. 16, 2020, [Online]. Available: https://d1wqtxts1xzle7.cloudfront.net/64999902/Tableu_Imager_dan_FTK_Imager.pdf?1606003446=&response-content-disposition=inline%3B+filename%3DCitra_Forensik_dari_barang_bukti_elektro.pdf&Expires=1609391012&Signature=ggq3RFljWBmjsEj5dsc0ammrrNiznpH1oGNpK57

[18] L. M. O. Campos, E. Gomes, and H. P. Martins, “Forensic Expertise in Storage Device USB Flash Drive: Procedures and Techniques for Evidence,” IEEE Lat. Am. Trans., vol. 14, no. 7, pp. 3427–3433, 2016, doi: 10.1109/TLA.2016.7587651.

[19] R. Ruuhwan, I. Riadi, and Y. Prayudi, “Penerapan Integrated Digital Forensic Investigation Framework v2 (IDFIF) pada Proses Investigasi Smartphone,” J. Edukasi dan Penelit. Inform., 2016, doi: 10.26418/jp.v2i1.14369.

[20] R. Umar, I. Riadi, and G. M. Zamroni, “Mobile forensic tools evaluation for digital crime investigation,” Int. J. Adv. Sci. Eng. Inf. Technol., vol. 8, no. 3, pp. 949–955, 2018, doi: 10.18517/ijaseit.8.3.3591.

[21] W. Jo, H. Chang, and T. Shon, “Digital forensic approach for file recovery in Unix systems: Research of data recovery on Unix file system,” Proc. 2016 IEEE Inf. Technol. Networking, Electron. Autom. Control Conf. ITNEC 2016, pp. 562–565, 2016, doi: 10.1109/ITNEC.2016.7560423.

[22] 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.

[23] Anton Yudhana, Abdul Fadlil, and M. R. Setyawan, “Analysis of Skype Digital Evidence Recovery based on Android Smartphones Using the NIST Framework,” J. RESTI (Rekayasa Sist. dan Teknol. Informasi), vol. 4, no. 4, pp. 682–690, 2020, doi: 10.29207/resti.v4i4.2093.

[24] I. A. Plianda and R. Indrayani, “Analisa dan Perbandingan Performa Tools Forensik Digital pada Smartphone Android menggunakan Instant Messaging Whatsapp,” J. Media Inform. Budidarma, vol. 6, no. 1, p. 500, 2022, doi: 10.30865/mib.v6i1.3487.

[25] W. Pranoto, “Penerapan Metode Live Forensics Untuk Akuisisi Pada Solid State Drive (SSD) NVMe Fungsi TRIM,” 2020.