TEKNOKOM : Jurnal Teknologi dan Rekayasa Sistem Komputer
Vol. 5, No. 2, September 2022, pp. 149 - 154
ISSN: 2686-3219, DOI: 10.31943/teknokom. v5i2.84

THE COMPARATIVE STUDY ANALYSIS LOGICAL FILES RECOVERY AND LOW LEVEL FILES RECOVERY USING DIGITAL FORENSIC METHODS

Rahmat Hidayat[1], Marza Ihsan Marzuki[2], Yuliarman Saragih[3], Ibrahim[4], Edmund Ucok Armin[5], Safrian Andromeda[6], Imam Budi Santoso[7], Suroyo[8]

[1]Department of Electrical Engineering, Universitas Singaperbangsa Karawang, Indonesia
[2]Department of Master of Electrical Engineering, Universitas Mercu Buana, Indonesia
[3]Department of Electrical Engineering, Universitas Singaperbangsa Karawang, Indonesia
[4]Department of Electrical Engineering, Universitas Singaperbangsa Karawang, Indonesia
[5]Department of Electrical Engineering, Universitas Singaperbangsa Karawang, Indonesia
[6]Department of Electrical Engineering, Universitas Singaperbangsa Karawang, Indonesia
[7]Faculty of Law, Universitas Singaperbangsa Karawang, Indonesia
[8]Faculty of Management, STIE Tribuana, Indonesia

ARTICLE INFO

History of the article:
Received September 16, 2022
Revised October 14, 2022
Accepted October 16, 2022
Published November 11,2022

Keywords:
File Recovery
Digital Forensics
Data
Technology

ABSTRACT

The development of application and network technology is currently so rapid. This technology is widely used as a solution to overcome data inspection problems in the field of Digital Forensics. The importance of Digital Forensics as evidence, especially on computers and mobile devices, is increasing, along with the rapid use of these mobile devices in daily communication. Data and files on computers and smartphones can be deleted intentionally or unintentionally. To recover the data, it is necessary to have Files Recovery. Furthermore, Logical Files Recovery can be made through password encryption, obtained through hack/attack password applications such as Password or even hacked with the "RecoveryMyFile" application. In addition, a search with a file that has a password description can be done. One of the file recovery applications that can be used is the Agent ransack search application, which is more powerful and convenient than Windows Search, which is more complicated if you need to search faster, indexing needs to be done, and restarts. By using Files Recovery analysis, the development of file or data deletion crimes can be overcome with increasingly rapid and advanced information technology, in this case through applications that can be used for file recovery and to restore deleted files.

Correspondece:
Rahmat Hidayat,
Department of Electrical Engineering,
Universitas Singaperbangsa Karawang,
Email :
rahmat.hidayat@staff.unsika.ac.id

INTRODUCTION

Along with the development of the era, digital technology is currently developing rapidly. At the same time, the development of hardware and software to provide mobile forensics investigation has been achieved. The development of application and network technology is currently very rapid. This technology is widely used as a solution to overcome data inspection problems in the field of Digital forensics [1]. The importance of Digital forensics as evidence especially files recovery related to the deletion of files or data to eliminate evidence of the crime is increasing, along with the rapid use of computer and mobile devices in communication and work tasks [2].

In cases involving computers and smartphones, investigators need to carry out computer and mobile forensics. Computer and Mobile forensics is a branch of digital forensics that studies how to recover evidence from computers and smartphones. Investigators will conduct a forensic analysis of smartphone devices using forensic tools with a methodology that has been forensically tested so that the analysis results are valid before the law and can be used as evidence [3].

In general, Digital Forensics is defined as the analysis of data, such as audio, and video which is obtained after the examination of electronic devices, to assist legal proceedings. Nowadays, with the advancement of technology, electronic devices are increasingly diverse such as tablets, flash memory, and memory cards. At the same time, the storage capacity of devices is increasing day by day. People use these devices extensively in many areas such as facilitating their work and keeping up with social circles. It is a critical issue to properly store and analyze this increased data in an electronic environment [4, 5].

Digital forensics aims to examine these devices and data to assist legal proceedings. When a forensic analysis is performed, the data on the device must be evaluated as unchanged and not destroyed. The results obtained can be used in the judicial process under these conditions. Digital forensics is divided into sub-disciplines as given among them are a) Computer Forensics, b) Mobile Forensics, c) Memory Forensics, d) Network Forensics, e) Malware Forensics, and f) OS (Operating System) Forensics [6-8].

The investigation process in Digital forensics is modeled with 4 main steps, including, 1) Assess which consists of Notifying and acquiring Authorization, reviewing policies and law, identifying team members, conducting assessment, Prepare for evident acquisition. 2) Acquire which consists of Build Investigation toolkit, Collect the data, Store, and achieve. 3) Analyze which consists of analyzing network data, analyzing host data, Analyze storage media. 4) Reporting which consists of gathering and Organizing, Write the report [9, 10]. This investigation process can be done in Files Recovery [11, 12].

Various kinds of tools that can be used to help the file recovery process include agent ransack, autopsy, RecoveryMyFile, recovered. wonder share, cleaner, clever files, and many more. These tools are tools to help uncover files that were intentionally deleted or deleted by individuals who intentionally deleted them to eliminate evidence of a crime.

Files Recovery in question aims to restore deleted data or files. In this all-digital world, many criminals delete data or files of evidence of their crimes to avoid punishment and lawsuits. Therefore, there is a need for a file recovery method or process to handle criminal cases in the digital world. However, the drawback of this method is that every deleted file, either on a computer or other device, has a period that is difficult to analyze and serve as data. Therefore, an investigator must carry out further analysis of the data obtained so that the data obtained becomes valid as evidence in the trial and can be brought to court [13].

Therefore, there is a need for a comparative study analysis of logical file recovery and low-level file recovery using digital forensics methods. Files Recovery, in the world of digital forensics and computers, is a branch of forensic and computer science that aims to identify, analyze, preserve, and recover valid digital evidence on computers, smartphones, as well as other devices and applications. The Files Recovery method can also be used as a process that can reveal evidence from a criminal case [14].

RESEARCH METHOD

The digital forensic method is a digital process by using analysis using software or applications to search for evidence directly and validly, in this case, the data sought can use the Files Recovery process. File Recovery in question aims to restore deleted data or files. In this all-digital world, many criminals delete data or files of evidence of their crimes to avoid punishment and lawsuits. Therefore, there is a need for a file recovery method or process to handle criminal cases in the digital world [15].

However, the drawback of this method is that every deleted file, either on a computer or other device, has a period that is difficult to analyze and serve as data. Therefore, an investigator must carry out further analysis of the data obtained so that the data obtained becomes valid as evidence in the trial and can be brought to court. In addition, the method in this study, there are several conditions and scenarios used in searching for data, namely analysis of logical files recovery and Analysis of delete/lost/low-level files recovery delete/lost/low-level files recovery.

Analysis of logical files recovery

1) Protect and encrypt your word document.
2) Save the file on the USB.
3) Search for files on the USB using the index in the window using the keywords listed in the word. Search for the keywords you are looking for so that they can be detected
4) Do a file search on the USB if you use an application, for example, agent ransack? https://www.mythicsoft.com/agentransack/
5) The password can be detected, so it is necessary to open the protected word file first. Can use the application: password recovery kit from pass ware https://www.passware.com/kit-basic/freedemo/

6) 6) Make comparisons in determining the results between using the index window and the transact agent.

Analysis of delete/lost/low-level files recovery delete/lost/low-level files recovery

Analysis of delete/lost/low-level files recovery delete/lost/low-level files recovery, is with the following steps:

a. Backup data on your USB
b. Performing data deletion on the USB with three levels:
   1) level 1 only deletes all files by doing a quick format on the USB
   2) level 2, by removing using a low format
   3) level by deleting using third-party apps to delete permanently.
c. Perform the analysis using one of the following applications;
   1) http://www.recovermyfiles.com/data-recovery software-download.php
   2) https://www.ccleaner.com/recuva
   3) https://www.cleverfiles.com/data-recovery-software.html
   4) https://recoverit.wondershare.com https://www.autopsy.com/
   5) Comparing the difference in the recovery results based on the three different levels mentioned above.

RESULTS AND DISCUSSION
Performing logical file recovery analysis

a. With word files that are encrypted or protected with a password, the file search results either with windows search or with the agent ransack application, the file cannot be found/detected, as shown in figure 1 for windows search and figure 2 with the agent ransack application.

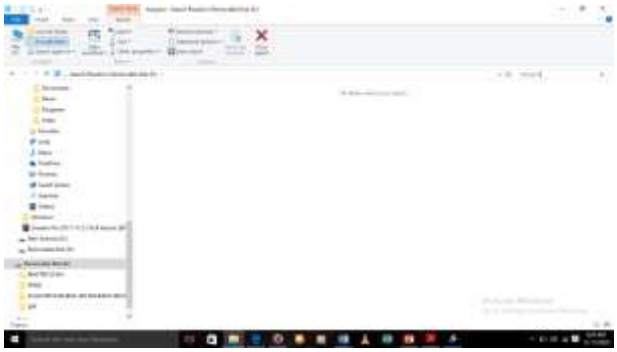

Figure 1. Search using Window search.

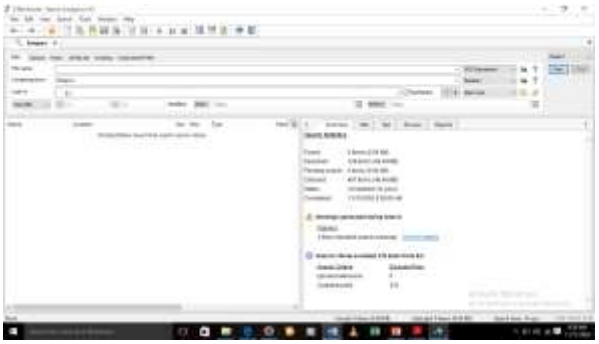

Figure 2. Search using the agent ransack application

a. Password encryption cannot be found by the “password recovery” application using the free version of the Password application, you may have to use a paid application. figure 3 shows the password cannot be detected using the free version of the Password application.

Figure 3. Password cannot be detected using the free version of the password application

b. Assuming Password can be described, file search can be continued as before, search with Windows and with Agent ransack application file can be found, as shown in Figure 4 for searching using windows search and figure 5 for searching using agent ransack application.

Figure 4. Search using windows

Figure 5. Search using the Agent ransack application

From figure 4 and figure 5, the results of the analysis are as follows: 1) Encrypted file search cannot be detected either with windows search or with transack agents, 2) In this experiment, it is said that the passware application used cannot hack password encryption in word files, maybe because it uses the free version of the application. Maybe you have to use a paid application, 3) It is assumed that the password has been described, then the search for files with the keywords contained in the word file can be done with windows search or with Agentransack, 4) Agentransack is more convenient to use because there is no need for indexing compared to windows search, so the display also displays more search results on Agentransack than on Window search.

Analyze delete/lost/low-level files recovery

Level 1: Lost files with Quick Format File Recovery with the "RecoveryMyFile" application or with "Recuva": File results can be recovered and can be opened even though the password is encrypted, as shown in the following screenshot:

Figure 6 and Figure 7 show the analysis and capture results with RecoveryMyFile.

Figure 6. The result of the recovery lost files with a quick format using the RecoveryMyFile application (a)

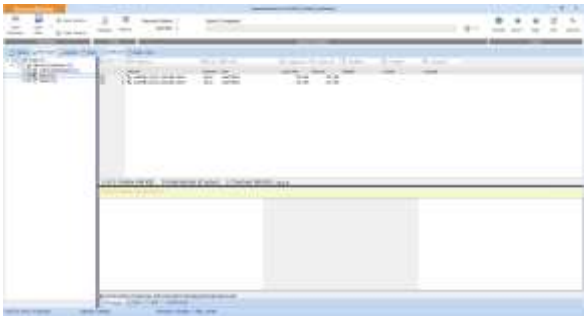

Figure 7.The result of the recovery lost files with a quick format using the RecoveryMyFile application (b)

Figure 8 shows the analysis and capture with Recuva.

Figure 8.The results of recovery lost files with a quick format using the Recuva application

Level 2: Lost files with Low Format: File Recovery with the "RecoveryMyFile" application which can be seen in figure 9 or with "Recuva": The result of the file cannot be recovered which can be seen in figure 10.

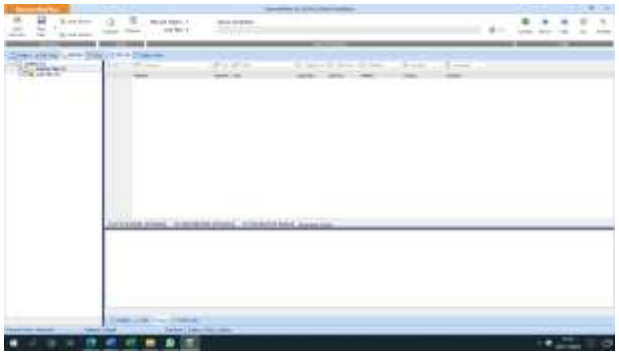

Figure 9.The result of recovering lost files with low format using the RecoveryMyFile application

Figure 10.The result of recovering lost files with low format using the RecoveryMyFile application

Level 3: Lost files by erasing using the "super eraser File Recovery" application with the "RecoveryMyFile" application which can be seen in figure 11 or with "Recuva": File results cannot be recovered which can be seen in figure 12.

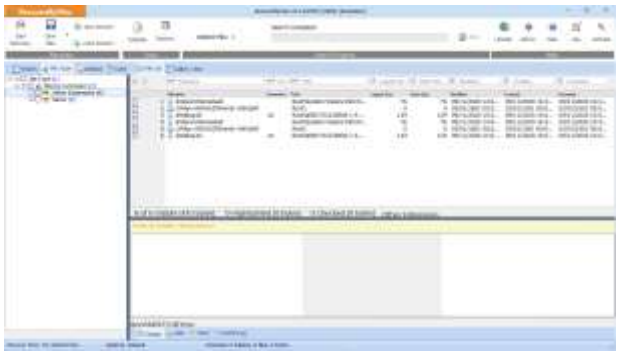

Figure 11.Super eraser File Recovery display with RecoveryMyFile Application

Figure 12.Display Results Files cannot be recovered in the Recuva application

From Figure 11 and Figure 12, the results of the analysis are as follows: 1) By using the RecoveryMyfile application, deleting files with level 1, namely Quick Format, files can be recovered and opened even though the file is encrypted, so RecoveryMyFile can simultaneously recover files and hack encryption passwords. 2) At Levels 2 and 3, the RecoveryMyFile application cannot recover deleted files.

CONCLUSION

the results of logical files recovery analysis, Files that are encrypted or protected with a password, will not be detected by searching for files either in Windows Search or with the Agent ransack application. Furthermore, Logical Files Recovery can be done through password encryption, which can be obtained through hack/attack password applications such as passware or even hacked with the “RecoveryMyFile” application. In addition, a search with a file that has a password description can be done.

One of the file recovery applications that can be used is the Agent ransack search application, which is more powerful and convenient than Windows Search, which is more complicated if you need to search faster because indexing needs to be done and needs to be restarted. Deleted files can be recovered only at level 1, namely Quick Format, while level 2 and Level 3 deleted files cannot be recovered, even with the recoveryMyfile application. It is hoped that by using File Recovery analysis, the development of the crime of deleting files or data can be overcome with increasingly rapid and advanced information technology, in this case through applications that can be used for file recovery and to restore deleted files.

REFERENCES

[1] T. E. Bracewell and C. Jones, "The use of simulated crime scenes in teaching undergraduate forensic sciences: Implementing an active learning approach to forensics," Science & Justice, 2022, doi: 10.1016/j.scijus.2022.08.003.

[2] R. Buyya, C. S. Yeo, S. Venugopal, J. Broberg, and I. Brandic, "Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility," Future Generation computer systems, vol. 25, no. 6, pp. 599-616, 2009.

[3] T. Holt and D. S. Dolliver, "Exploring digital evidence recognition among front-line law enforcement officers at fatal crash scenes," Forensic Science International: Digital Investigation, vol. 37, 2021, doi: 10.1016/j.fsidi.2021.301167.

[4] Y. Azzery, N. Dwi Mulyanto, and T. Hidayat, "Memory Forensic Development and Challenges in Identifying Digital Crime : A Review," Teknokom, vol. 5, no. 1, pp. 96-102, 2022, doi: 10.31943/teknokom.v5i1.73.

[5] F. Holz, M. F. Saulich, A. S. Schroder, C. G. Birngruber, M. A. Verhoff, and S. Plenzig, "Death abroad: Medico-legal autopsy results of repatriated corpses: A retrospective analysis of cases at the Department of Legal Medicine in Frankfurt am Main," Forensic Sci Int, vol. 310, p. 110257, May 2020, doi: 10.1016/j.forsciint.2020.110257.

[6] G. Horsman, "Digital evidence and the crime scene," Sci Justice, vol. 61, no. 6, pp. 761-770, Nov 2021, doi: 10.1016/j.scijus.2021.10.003.

[7] C. Shi, J. C. Dumville, H. Juwale, C. Moran, and R. Atkinson, "Evidence assessing the development, evaluation and implementation of digital health technologies in wound care: A rapid scoping review," J Tissue Viability, Sep 27 2022, doi: 10.1016/j.jtv.2022.09.006.

[8] G. Tutt and S. Hoffmann, "Forensics in motion - Historic vehicles, genuine or fake," Forensic Sci Int Synerg, vol. 4, p. 100218, 2022, doi: 10.1016/j.fsisyn.2022.100218.

[9] S. Park et al., "A comparative study on data protection legislations and government standards to implement Digital Forensic Readiness as mandatory requirement," Digital Investigation, vol. 24, pp. S93-S100, 2018, doi: 10.1016/j.diin.2018.01.012.

[10] A. O. Philip and R. K. Saravanaguru, "Smart contract based digital evidence management framework over blockchain for vehicle accident investigation in IoV era," Journal of King Saud University - Computer and Information Sciences, vol. 34, no. 7, pp. 4031-4046, 2022, doi: 10.1016/j.jksuci.2022.06.001.

[11] D. Seddiki, S. G. Galán, J. E. M. Expósito, M. V. Ibañez, T. Marciniak, and R. J. Pérez de Prado, "Sustainable expert virtual machine migration in dynamic clouds," Computers and Electrical Engineering, vol. 102, p. 108257, 2022/09/01/ 2022, doi: https://doi.org/10.1016/j.compeleceng.2022.108257.

[12] M. Arif, A. K. Kiani, and J. Qadir, "Machine learning based optimized live virtual machine migration over WAN links," Telecommunication Systems, vol. 64, no. 2, pp. 245-257, 2017.

[13] D. Scheffer et al., "Active mixture of serum-circulating small molecules selectively inhibits proliferation and triggers apoptosis in cancer cells via induction of ER stress," Cell Signal, vol. 65, p. 109426, Jan 2020, doi: 10.1016/j.cellsig.2019.109426.

[14] M. Aiash, G. Mapp, and O. Gemikonakli, "Secure live virtual machines migration: issues and solutions," in 2014 28th International Conference on Advanced Information Networking and Applications Workshops, 2014: IEEE, pp. 160-165.

[15] F. Xu, F. Liu, L. Liu, H. Jin, B. Li, and B. Li, "iAware: Making live migration of virtual machines interference-aware in the cloud," IEEE Transactions on Computers, vol. 63, no. 12, pp. 3012-3025, 2013.