International Journal of Engineering & Technology, 7 (4.7) (2018) 445-448

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

Comparative Analysis Of Applications OSforensics, GetDataBack, Genius and Diskdigger On Digital Data Recovery in the Computer Device

Arif Hidayat*, Sudarmaji, Dharmawan, Dedi Irawan, Lilik Joko Susanto, Mustika, Hadi Pranoto

Universitas Muhammadiyah Metro, Lampung, Indonesia
**Corresponding author E-mail: androidarifhidayat@gmail.com*

Abstract

In the use of computer devices that are done in recent use for data processing in the form of text, images or video that can be done easily and quickly. But in reality, there are events where the work, in the form of computer files, can be lost so that the required files are missing from the storage media in the computer. In this research will be discussed and presented a comparative analysis of four software for recovery of data that has been deleted. The applications used are OSforensics, GetDataBack, Disk Genius and Diskdigger. The capabilities of such applications in the recovery of deleted data have been tested and analyzed in flash drives. Based on the tests that have been done indicates that the fourth this application can work well in terms of finding deleted data. In addition, this application is also able to recover data or retrieve the already deleted.

Keywords: *Digital Data Recovery, OSforensics, GetDataBack, Disk Genius, Diskdigger*

1. Introduction

Advances in technology such as mass media, online games, and social media such as facebook, twitter, Instagram has become part of the needs of life in today's society, especially the younger generation. One of the negative impacts of this technological advancement is the misuse of such technology for the crime. Crimes related to the use of computers on such media are usually known by name cybercrime. Cybercrime is defined as an unlawful act that utilizes computer technology based on the sophistication of internet technology development. Although cybercrime crime generally refers to criminal activity with computers or computer networks as its main element, the term is also used for traditional criminal activities in which a computer or computer network is used to facilitate or enable the crime to occur.

Examples of cybercrime crimes in which computers as a tool are spamming and crimes against copyright and intellectual property. Examples of cybercrime crimes in which computers are targeted are illegal access (tricking access control), malware and DoS attacks. An example of a cybercrime crime in which the computer is its place is an identity fraud. While the example of traditional crime with the computer as a tool is child pornography and online gambling. Cybercrime behavior is certainly very detrimental to its victims and contrary to the law. To punish the cybercrime the authorities will usually look for some evidence. One of the evidence is the computer used by the offender.

The data contained in the computer will be taken as evidence in punishing cybercrime perpetrators. Basically, files deleted or deleted from our computer are not completely lost, there is a system that is responsible for accommodating the deleted files, but sometimes we forget and ignore them, so the files seem like permanent lost. In practice, the data inside the computer has been removed by the perpetrator before the computer is seized by the authorities. In this case is required software to recover the deleted data. Currently, there are many applications contained in the market that can be used to restore the data that already removed that is OSforensics, GetDataBack, Disk Genius and Diskdigger. To know the ability of the four applications, the authors do research with the title "Comparison Analysis OSforensics Applications, GetDataBack, Disk Genius and Diskdigger against Digital Data Recovery on Computer Devices".

There has been much research done on digital data recovery analysis that is, the research-like as done by Handrizal in 2017 entitled Comparison Analysis Toolkit Puran File Recovery, Glary Undelete and Recuva Data Recovery for Digital Forensics. In this study discusses the comparative analysis of the three digital forensic toolkits for data recovery scenario that has been deleted. Analysis begins with 1) format flash drive, 2) fill out the data on the flash drive, 3) delete all data in the flash drive, 4) Empty recycle bin, 5) Use toolkit. The results of the comparison show that the three toolkits can work well in terms of finding deleted data or recovering the deleted data.

Another second study refers to the issues raised by Pastima Simanjuntak and Winarto in 2017 entitled Comparative Analysis of Recovery and Recuva Recovery Applications against Windows Data Recovery. In this study discusses the comparison between the two software. In this study showed that results time left Recuva as Software better than Pandora Recovery. The likelihood of being an important factor why Recuva is much preferred by users is the way its features are better than Pandora Recovery. In addition, this research also states that Recuva can restore files that have been permanently deleted and temporarily, but can not restore formatted data, lost due to viruses, Partitioned and damaged Files. However for Pandora Recovery can restore all data that has been formatted, lost due to viruses, Partitioned and corrupted Files. Temporarily deleted files can be restored easily by restoring these files when they are in the recyclebin.

Copyright © 2018 Arif Hidayat. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Another third study refers to the issues raised by Vidila Rosalina, Andri Suhendarsah and M. Natsir in 2016 entitled Data Recovery Analysis Using Forensic Software: Winhex and X-Ways Forensic. In this study discusses forensic software: winhex and x-ways forensic that can perform data recovery with more perfect. The conclusion of the research is the use of forensic software: winhex and x-ways forensic has many advantages in data recovery so that it can assist law enforcement in completing Rules of Evidence and Chain of Custody requirements.

Another fourth study refers to the issues raised by Aan Widayat Wisnu Budi and Muhammad Kusban in 2015 entitled Computer Forensic Analysis to Support the Process of Investigation in the Crime Case. This elitist pen provides an overview of the application of certain methods in tracing the evidence leads to the crime of the suspect. This research and analysis m contrasting initial or early hypotheses with post-process analysis recovery data, whether the initial hypothesis can be taken into a final conclusion or no. The final conclusion is expected to be useful information for the process of investigation is being done.

Based on the results of research on recover digital data that has been described above, then conducted further research with the title "Comparative Analysis Of Applications *OSforensics*, *GetDataDack*, *Genius* and *Diskdigger* On Digital Data Recovery In The Computer Device". The object used in this research is digital data recovery on computer devices. Applications used for testing in terms of comparative analysis are Osforensics, GetDataBack, Disk Genius and Diskdigger. The output that resulted in the results of analysis and comparison of applications Osforensics, GetDataBack, Disk Genius And Diskdigger to taking digital data recovery in the computer device.

2. Methodology

Method the research used is the experimental method. According to Sumantri (1999: 157) the experimental method is a demand of the development of science and technology in order to produce a product that can be enjoyed by society safely and in learning involving students by experiencing and proving themselves the process and result of the experiment. As for The research flow that writers do that can be seen in the following figure 1.

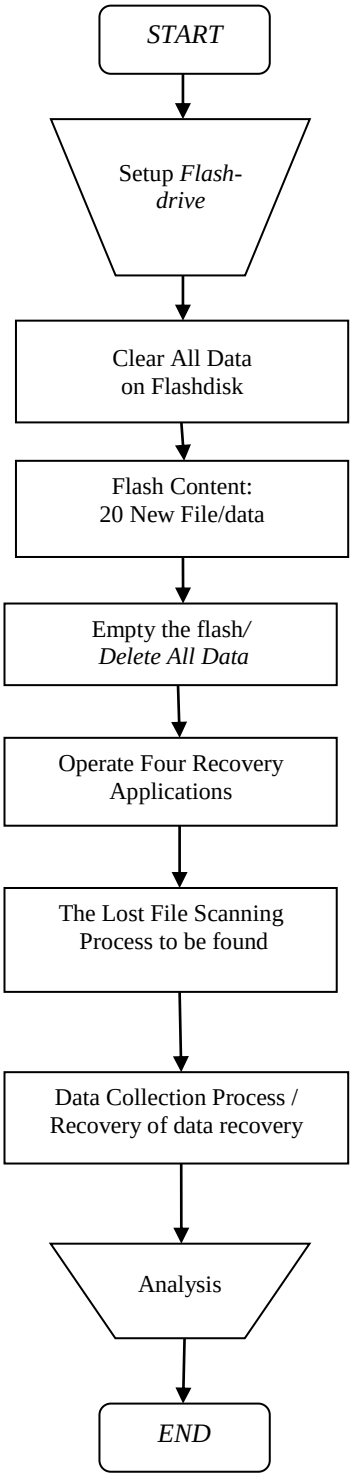


Figure 1: Flowchart of Research

3. Result and Discussion

Implementation or application of OSforensics, GetDataBack , Disk Genius and Diskdigger has done on Windows Operating System 8. These four applications are software freeware / can be downloaded for free. After four software is downloaded and then installed. Once installed in the last stage of testing the four data recovery applications. Need to know fourth testing this application is done to find out how the performance of applications in search data that has been deleted in a flash drive. In this test will be seen the results based on the amount of data that can be scanned and the amount of data that can be recovered. The first stage of testing will be done using the OSforensics application. Further testing continued with GetDataBack application, then next

with testing application Disk Genius and lastly with Diskdigger. The testing stages for each application are as follows: 1)Remove the flash drive, 2) Copy twenty files from drive D:/ to flash drive, 3) Delete all data in the flash drive, 4) Empty the recycle bin, 5) Operate Applications Recovery

3.1 Testing OSforensics Application

On testing with OSforensics done with the following steps:

1. Insert the USB flash drive into the USB port and then can be checked, even so flash drive empty.
2. Run the application OSforensics, then after choose File menu search Deleted will appear a new window, please on the Disk tab select flash and press the search button to start the search.
3. Will appear the results of data ever deleted on the flash disk drive. Ever the delete data appear and a total of 20 items file.

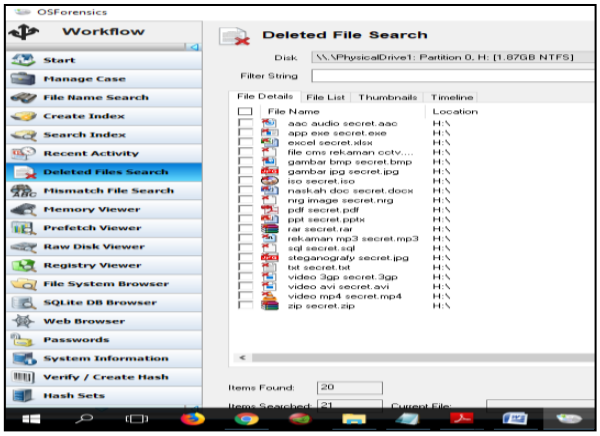


Figure 2: Results of Data Recovery Using OSForensics Application

4. The app wants to more clearly click the Thumbnail tab in the Deleted File Search window. From the results of this test shows that data whoever in delete 20 items can reappear and can be retrieved on file 20 items files.

3.2 Testing GetDataBack Application

On testing with GetDataBack done with the following steps:

1. Insert the USB flash drive into the USB por and then right click on the drive Flashdisk → Select Properties, After that will appear File System: NTFS. Therefore if it appears File System: NTFS then the author wait will be application GetDataBack for NTFS funds when the FAT file system then the authors use the Get Databack for FAT.
2. Run the GetDataBack app, after it on the Select Drive window select Flash Drive, then click Next. Then in the window Select the file system to select the color green (containing the data you want recovered sectors), application GetDataBack will bring up the recovery or called the Recovery Tree. The data that is recovered if successful will appear. In this test succeeded 100% lost data successfully withdrawn and show with the total number of 20 items files.
3. If you want the data to be lifted to another drive device then it can be done by blocking file then right click select copy then navigate the free storage location is not important in flashdisk in the recovery.

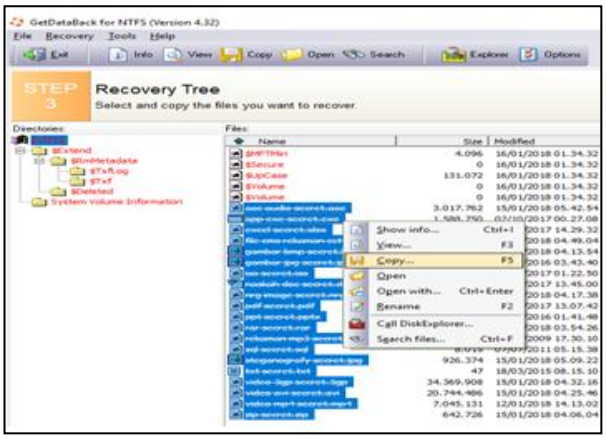


Figure 3: View Copy File from Recovery Tree In Applications GetDataBack for NTFS

3.3 Testing Disk Genius Application

On testing with Disk Genius done with the following steps:

1. Insert USB flash Disk to the USB port and run the Disk Genius app. Once open Disk Genius application then select flash drive and right click select Recover Lost Files or Formatted Partition.
2. Then select Recover Deleted files and click Start to begin the recover the data that had been erased, a right turn up results from livelihoods files that have been deleted.
3. If you want to do the data appointment, as for how to click all data Partitions file then right click select Copy To Desktop. After that point save it to Drive other than Flashdisk.

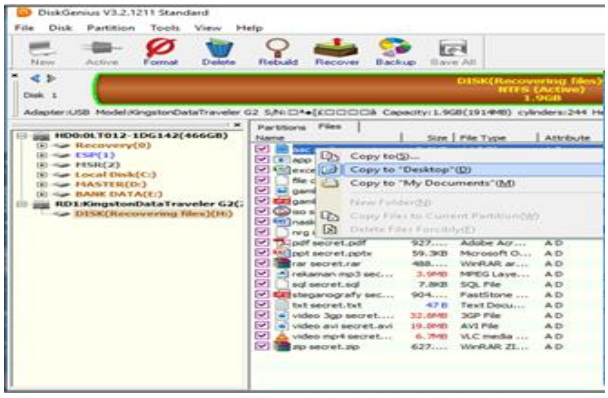


Figure 4: Display Step Appointment Data Recovery findings in the Disk Genius Application

4. Copying process will emerge Files Into Folders "Lift Results disk Genius" will appear then acyl appointment results in the Application Data Recovery Disk Genius totaling 20 items of different file types the data type.

3.4 Testing DiskDigger Application

In the test with DiskDigger done with the following steps:

1. Insert USB flash Disk drive to the USB port and run the DiskDigger app. In this step, we will get a view on the application screen like picture 24. Once open click the flash drive and click next to continue. Then after selecting the select partition to scan then it will appear scan mode selection recovery Diskdigger application.
2. From scanning results using disk digger application, obtained data recovery results and the results are displayed on the Search Results tab window.
3. Then, after the discovery of the file can be followed by removal of the file, by right-clicking a file or block that would in the lift and then select Restore selected files. Followed by determining the storage location, keep in mind that any data

removal for the location of the appointment should not be done on the recovery drive, that means we save it in other than the flash drive. There is this test the removal of digital data, the authors save it p Drive E: /

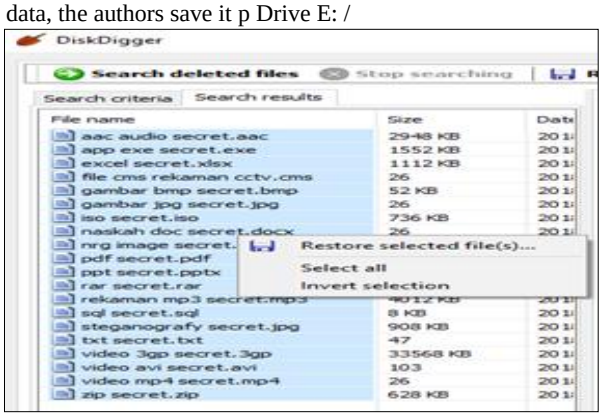


Figure 5: Display Step Appointment Digital Data Recovery Using DiskDigger Application

4. The results in Figure 4. below illustrate the results of digital recovery data recovery using the DiskDigger application. The result of the successful file in the lift is 20 items file.

3.5 Application Testing Results

From the test that has been done using a USB flash drive as mentioned above, the results obtained as shown in table 1 below:

Table 1: Comparison of Osforensics Applications, GetData Back, Disk genius and Diskdigger

No	Parameter	*OS forensics*	*GetDataBack*	*Disk genius*	*Diskdigger*
1.	The amount of data **successfully Scanned**	20 items file	20 items file	20 items file	20 items file
2.	The amount of data **successfully Recovery**	20 items file	20 items file	20 items file	20 items file

Based on Table 1 and Table 2 it is known that the four applications used can find all files that have been deleted and can recover all the files that have been deleted. In this experiment, the number of deleted files is 20 files for all four applications.

Table 2: Description 20 File Succesfully Recovery

No	Nama File Name	Data Type	Size	Desription
1	Aac Audio Secret	.aac	2.948 KB	Audio File
2	App Exe Secret	.exe	1.552 KB	Exe File
3	Excel Secret	.xls	1.109 KB	Office/ Excel File
4	File CMS Rekaman Cctv	.cms	58.072 KB	Record CCTV File
5	Gambar Bmp Secret	.bmp	51 KB	Image File
6	Gambar Jpg Secret	.jpg	417 KB	Image File
7	Iso Secret	.iso	736 KB	ISO File
8	Documents Doc Secret	.doc	108 KB	Document File
9	Nrg Image Secret	.nrg	441 KB	NRG File
10	Pdf Secret	.pdf	928 KB	Pdf File
11	Ppt Secret	.ppt	60 KB	Office/ ppt File
12	Rar Secret	.rar	488 KB	Rar File
13	Record mp3 Secret	.mp3	4.012 KB	Musics/ mp3 file
14	Sql Secret	.sql	8 KB	Database/ sql file
15	Steganografi Secret	.jpg	905 KB	Steganografi file
16	Txt Secret	.txt	1 KB	Text File
17	Video 3gp Secret	.3gp	33.565 KB	Video File
18	Video Avi Secret	.avi	20.259 KB	Video File
19	Video mp4 Secret	.mp4	6.881 KB	Video File
20	Zip Secret	.zip	628 KB	Zip File

4. Conclusion

Based on research that has been done above can take the conclusion, among other things:

a. From a generated research comparison analysis of Osforensics applications, GetDataBack, Disk genius and Diskdigger against digital data recovery on computer devices
b. Application OSforensics, GetDataBack, Disk Genius and Diskdigger can find all deleted files in a flash drive although it has been emptied from the recycle bin.
c. Application OSforensics, GetDataBack, Disk Genius and Diskdigger can recover all deleted files in a flash drive.

References

[1] EMS, Tim, (2009), *Mengatasi Data Hilang dan Serangan Virus*. Penerbit: Elex Media Komputindo.
[2] Sulianta, Feri, (2008), *Komputer Forensik*, Penerbit: Elex Media Komputindo.
[3] Simajuntak, P. (2017). *Analisis Perbandingan Aplikasi Pandora Recovery Dan Recuva Terhadap Pengembalian Data Windows*. Journal Information System Development (ISD), 2(1).
[4] Handrizal, H. (2017). *Analisis Perbandingan Toolkit Puran File Recovery, Glary Undelete Dan Recuva Data Recovery Untuk Digital Forensik*. J-SAKTI (Jurnal Sains Komputer dan Informatika), 1(1), 84-94.
[5] Mirk, Steven,(2015) *File Data Recovery Secrets: Tips and Tricks for Recovering Data*. Penerbit: Lulu Press, Inc.
[6] Blank, Mathew, (2014). *File Data Recovery: PC Hard Drive Data Recovery, USB Data Recovery, Mac Data Recovery, Android Data Recovery, Data Recovery Services*. Penerbit: CreateSpace Independent Publishing Platform.
[7] Hidayat, A. (2017). Konfigurasi Server Cloud Storage pada Jaringan LAN pada LAB Diploma III Manajemen Informatika UM Metro. *MIKROTIK: Jurnal Manajemen Informatika*, *7*(1).
[8] Rosalina, V., Suhendarsah, A., & Natsir, M. (2017). ANALISIS DATA RECOVERY MENGGUNAKAN SOFTWARE FORENSIC: WINHEX AND X-WAYS FORENSIC. PROSISKO: Jurnal Pengembangan Riset dan Observasi Sistem Komputer, 3(1).
[9] Kripalani, S. H., & Gokhale, P. (2018). *U.S. Patent Application No. 15/664,841*.
[10] Bourbonnais, S., D'costa, A. F., Lau, Y. O., Li, X., Min, H., Su, G. & Zentgraf, C. (2018). *U.S. Patent Application No. 15/237,407*.
[11] Kortunov, D., Protassov, S. S., & Beloussov, S. M. (2018). *U.S. Patent No. 9,894,510*. Washington, DC: U.S. Patent and Trademark Office.
[12] Iorliam, A. (2018). Forensic Tools for Different Subdivisions. In *Fundamental Computing Forensics for Africa* (pp. 57-68). Springer, Cham.
[13] Ries, G., Salemi, E., & Alaya, S. B. (2018). *U.S. Patent No. 9,946,652*. Washington, DC: U.S. Patent and Trademark Office.
[14] Hidayat, A., (2018). COMPARATIVE ANALYSIS OF MIKROTIK SITE FILTER USING ADDRESS LIST TECHNIQUES, LAYER7 PROTOCOLS, WEB PROXY, MANGLE AND DNS STATIC. *International Journal of Engineering & Technology*, *7 (3.4)* 272-275