Computer Forensic Using Photorec for Secure Data Recovery Between Storage Media: a Proof of Concept

I Putu Agus Eka Pratama

[1] Department of Information Technology, Faculty of Engineering, Udayana University,
Jimbaran, Bali 80361, Indonesia.
*Corresponding Author:
Email: eka.pratama@unud.ac.id

Abstract*.*
Data plays the important role, so that data recovery and data security be prioritized. Computer users often lose their data due to personal errors or by attacks. Digital forensics has one sub-field called computer forensic, which has an important role in the process of secure data recovery. USB Flashdisk as the most widely used storage media has a probability of data loss. It is necessary to do computer forensic actions, especially secure data recovery, on it so that it can restore data securely to other media while protecting it by giving privilege root. In this research, computer forensic testing the 2781 files of various data formats that were erased on a 32 GB USB flash drive using Photorec. The media for collecting data recovery results using an Intel computer, 2 GB RAM, 1.8 GHz processor, the Linux operating system Xubuntu 20.04. Testing is carried out following the test scenarios that have been designed, then observed, recorded, and analyzed. Photorec places recovery data in 6 recup_dir subdirectories. Test results and analysis of the test results show that Photorec is a reliable tool for computer forensic, especially secure data recovery because it can restore 100% of data, accompanied by privilege root for all data recovery results, so they cannot be changed and deleted by an end-user without granted access.

Keywords: *Computer forensics, data, Industry 4.0, Photorec, secure data recovery.*

I. INTRODUCTION

Nowaday, data plays an important role in all aspects of human life: technology, Industry 4.0, Internet of Things, and internet services [1]. Because of data is so important, there are two main priorities, namely: 1.) Data security, 2.) Data recovery process. For data security, one of the main focuses is on data security in the data center, thus requiring the implementation of a data center room using the TIA-942 standard [2]. The second priority is the data recovery process, closely related to digital forensics along with data security challenges in the data recovery process. For this reason, it is necessary to pay attention to secure data recovery that is carried out between data storage media.

Secure data recovery is related to forensics and digital forensics. Forensic is defined as a scientific effort to collect, analyze, and present physical evidence in court, while digital forensics is the same thing in case studies related to digital technology, which is divided into computer forensics, mobile forensics, and network forensics [4].

Digital Forensic with one of its sub-fields called Computer Forensic, provides secure data recovery facilities to help restore lost data as well as secure it [5].

In the law field, data recovery in digital forensics and computer forensics helps investigators in the forensic process to find evidence that supports the course of a case investigation. For example digital forensic file conversations on Whatsapp in online fraud cases [6] and cybercrime cases with evidence of digital conversations on Line [7]. In the business world, data recovery plays a role in protecting the company's digital assets. Because it is so important, that data recovery is included in the Disaster Recovery Plan (DRP) [8][9] and Disaster Recovery Plan (DRP), both of which are based on the NIST SP 800-34 Framework [10].

Currently, there are a number of choices of data storage media with various storage capacities in it. The following Table 1 shows the data storage media, storage capacities, and descriptions for each storage media:

Table 1. Data Storage Media, Storage Capacities, and Descriptions

Data Storage Media	Capacity	Description
Floppy Disk	1.44MB	A 35-inch disk, as of 2020 is rarely used.
CD-ROM	650MB-800MB	Includes CD-R (one write) and CD-RW (multiple writes).
DVD-ROM	1.67GB-15.9GB	Includes DVD-R (one write) and DVD-RW (multiple writes).
Hard Drive	20GB-1TB	Optical hard drives are commonly used in computers.
ATA Flashcard	8MB-2GB	PCMCIA flash memory cards; measuring 85.6 x 54 x 5 mm.
USB Flashdisk	16MB-4GB	The most widely used storage media. Its size capacity is increasing, including those tested in this research.
Compact Flash Card	16MB-6 GB	Type 1 cards measure 43 x 36 x 3.3 mm, type 2 cards measure 43 x 36 x 5 mm.
Secure Digital (SD) Card	32MB-1GB	Meet the needs with the Secure Digital Music Initiative (SDMI), providing encrypted built-in data, from a size similar to MMC.
Memory Stick	16MB-2 GB	Includes Memory Stick (50 x 21.5 x 2.8 mm), Memory Stick Duo (3 1 x 20 x 1 6 mm), Memory Stick PRO, Memory Stick PRO Duo, some meet SDMI needs and provide built-in encryption.

Based on a number of data storage media options in Table 1 above, USB flash drives are the most widely used storage media by computer users. Data of computer users on USB Flashdisk media is often lost or damaged. Given that data is important for personal computer users and organizations in Industry 4.0, it is necessary to strive for a secure data recovery process.

There are eight previous studies that are related and become state of the art. Research from Yudhana describes a mobile forensics method based on guidelines from the National Institute of Standards of Technology (NIST), which produces data type headers in the form of deleted account names, deleted file types, and deleted timestamps [10]. Wollaston et al., in their paper, compared the data recovery functions of two forensic suites and three standalone non-forensic commercial applications, with the result that all tools had a comparable performance with respect to data recovery functions [11]. Sitompul et al., propose an Aho-Corasick parsing technique to read file attributes from the master file table (MFT), in order to examine the file condition, with the result that the file reconstruction process on the file system was performed successfully in 87.50% and string matching process average time was 0.32 second [12]. Bansal et al., describe the various methods and tools to recover data from Harddisk, how data recovery tools work, in what situation the data can lose permanently, and in what conditions data can be recovered [13]. On the other hand, Lazaridis et al., published their research on comparison and evaluation of several digital forensics tools on data recovery scenarios, in which it has been tested and evaluated in order to provide evidence regarding their capabilities in qualitative analysis and recovery of deleted data from various file systems [14]. The other research by Riskiyadi has described the reliability of digital forensic tools in uncovering cybercrime, to obtain digital evidence with integrity, reliability, and legality, using static forensic methods based on the National Institute of Justice (NIJ) framework, with case studies of cybercrime carding and electronic evidence flash disks using digital tools Forensic FTK Imager and Autopsy [15]. The testing of three digital forensics toolkits for data recovery scenarios that have been deleted (Puran File Recovery, Glary Undelete, Recuva Data Recovery) was conducted by Handrizal, in which these three toolkits can restore deleted data that has been tested and analyzed in a USB flash. drives [16]. The last, research by Riadi et al., compared the performance of forensic tools to restore deleted data (contacts, call logs, messages) that were used as evidence in court, using two smartphones and forensic tools (Wondershare dr. Fone for Android), Oxygen Forensics Suite 2014) with the NIST method [17].

Based on the state of the art above, this paper describes the testing of secure data recovery from the digital forensics perspective on USB Flashdisk media to a computer hard drive, using the Photorec tool. The test was carried out on a Toshiba L40 notebook (1.8 GHz processor, 2 GB RAM, 500 GB HDD, 64 bit), Linux Xubuntu 20.04, 2781 files of various data formats on a 32 GB Toshiba USB Flashdisk. Tests are carried out using predetermined test scenarios. The final objective of the study is to test the reliability of the selected Photorec tool in performing secure data recovery.

II. METHODS

This research was conducted privately in the author's home at Gianyar, Bali (Indonesia) during the Covid-19 pandemic, from June 2020 to December 2020. This research was carried out using experimental research method. The research steps were carried out according to the experimental research method, including: 1.)Identification of data problem cases, 2.)Identification of data extensions, 3.)Data recovery process based on conditions. The three steps are presented in the form of a flowchart diagram as shown in Fig. 1. below:

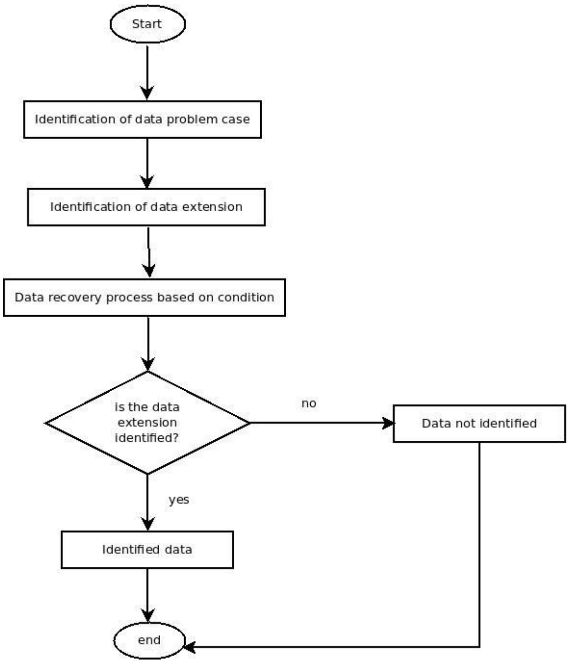
Start
Identification of data problem case
Identification of data extension
Data recovery process based on condition
is the data extension identified?
no
Data not identified
yes
Identified data
end

Fig. 1. Flowchart diagram

As shown in Fig. 1. above, the research steps start from identification of data problem cases, then continue with identification of data extensions, then proceed with data recovery process based on conditions. Then there is a condition whether the data extension is identified. If yes, then the data is identified, while if it is no, then the data is not identified.

III. RESULT AND DISCUSSION

Scenario Testing

The scenario testing used in this study is as follows: 1.)Provided a 32 GB USB Flashdisk with 2781 files (various data formats) as a data recovery target, plugged it into the computer, then checked the entire partition and found the location of the mounted USB Flashdisk partition. 2.)Run Photorec in Linux Terminal, detect USB Flashdisk, filesystem, a partition that is the target of recovery, and partition where data is saved from recovery. 3.)Perform testing, observe and record test results, analyze test results. 4.) Documentation of research results.

Testing

In this research, testing is carried out through the following set of processes below:

1.)After the USB Flashdisk as the recovery target is plugged in, then tested via the fdisk command to see the location of the USB flash drive partition that is mounted to the system.

```
certain-death@my-toshiba:~$ sudo fdisk -l

Disk /dev/sda: 465,78 GiB, 500107862016 bytes, 976773168 sectors
Disk model: ST500VT000-1DK14
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 4096 bytes
I/O size (minimum/optimal): 4096 bytes / 4096 bytes
Disklabel type: dos
Disk identifier: 0x7562af67
Perangkat  Boot   Start     Akhir    Sektor   Size Id Tipe
/dev/sda1  *       2048   1050623   1048576   512M  b W95 FAT32
/dev/sda2       1052670 976771071 975718402 465,3G  5 Extended
/dev/sda5       1052672 976771071 975718400 465,3G 83 Linux

Disk /dev/sdb: 28,93 GiB, 31037849600 bytes, 60620800 sectors
Disk model: TransMemory
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: dos
Disk identifier: 0x707f203b
Perangkat  Boot Start    Akhir   Sektor  Size Id Tipe
/dev/sdb1          63 60619103 60619041 28,9G  c W95 FAT32 (LBA)
certain-death@my-toshiba:~$
```

From the above test, it can be seen /dev/sda as the computer's hard disk partition and /dev/sdb as a USB flash partition mounted to the system.

2.)Photorec is run through the command in Linux Terminal with root access (sudo) as follows, to display a list of partitions on the computer:

```
certain-death@my-toshiba:~$ sudo /usr/bin/photorec
[sudo] password for certain-death:

PhotoRec 7.1, Data Recovery Utility, July 2019
Christophe GRENIER <grenier@cgsecurity.org>
https://www.cgsecurity.org

  PhotoRec is free software, and
comes with ABSOLUTELY NO WARRANTY.

Select a media (use Arrow keys, then press Enter):
>Disk /dev/sda - 500 GB / 465 GiB (RO) - ST500VT000-1DK142
 Disk /dev/sdb - 31 GB / 28 GiB (RO) - TOSHIBA TransMemory
```

USB flash media (/dev/sdb) is the target of data recovery in this research, to be moved to the computer hard disk partition (/dev/sda).

3.)Move the cursor to the USB flash disk partition in /dev/sdb, selecting the Proceed option. Photorec will reads the partition from the target recovery media (/dev/sdb) belonging to the USB Flashdisk, identified with the FAT32 filetype. Click the Search option.

4.)Photorec reads the filesystem type of the target partition, which is FAT32. Select the Other option. The recovery process is carried out through an unrecognized memory location on the FAT data, then select the Free option.

5.)Choose a location on the hard disk partition on the computer to accommodate the data recovery files, namely /home/certain-death/recovery. Point the cursor to the recovery sub directory. click the recovery sub directory then press C. The recovery process will start running. The recovery process was successful and finished well for 2781 files.

```
PhotoRec 7.1, Data Recovery Utility, July 2019
Disk /dev/sdb - 31 GB / 28 GiB (RO) - TOSHIBA TransMemory
     Partition                  Start        End    Size in sectors
   P FAT32                    0   0  1 29564  63 32   60549120

2781 files saved in /home/certain-death/recovery/recup_dir directory.
Recovery completed.
```

The data recovery results are stored in the /home/certain-death/recovery/ sub directory in six folders, namely: recup_dir.1, recup_dir.2, recup_dir.3, recup_dir.4, recup_dir.5, and recup_dir.6, as shown in Fig. 2. below:

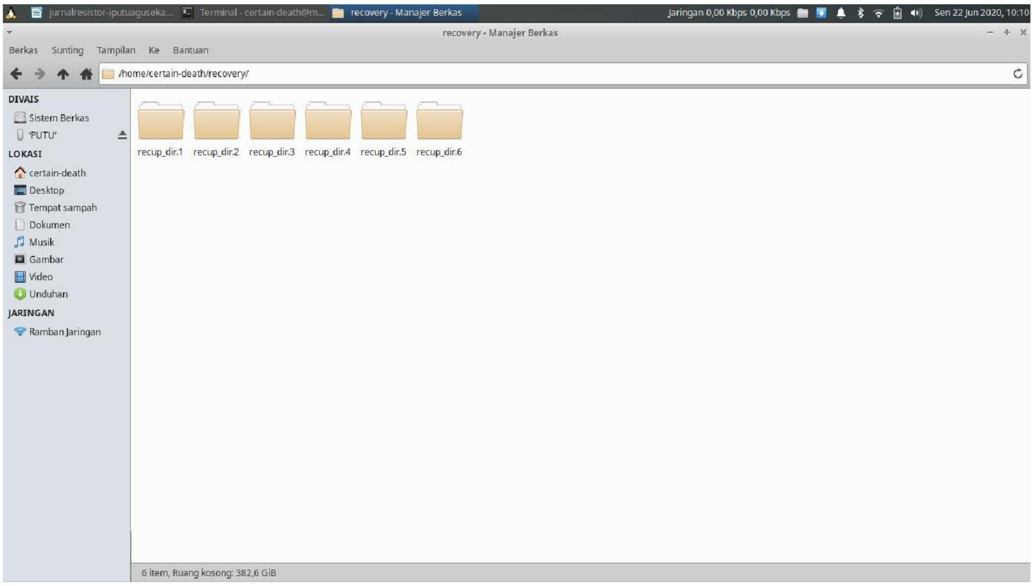

Fig. 2. Data recovery results

Discussion

All data (2781 files) can be recovered properly and read well. All recovered files have root ownership access (shown in some files only in recup_dir.1):

```
certain-death@my-toshiba:~/recovery/recup_dir.1$ ls -la
total 4639352
drwxr-xr-x 2 root          root             40960 Jun 22 09:55 .
drwxrwxr-x 8 certain-death certain-death     4096 Jun 22 10:05 ..
```

```
-rw-r--r-- 1 root           root              30113792 Jun 22 09:53
f14732192.bz2
-rw-r--r-- 1 root           root              61844672 Jun 22 09:53
f14791008.xz
-rw-r--r-- 1 root           root                   186 Jun 22 09:53
f14912128.png
-rw-r--r-- 1 root           root               3276800 Jun 22 09:53
f14917952_389_ds_base_snmp_1_3_9_1_10_el7.rpm
-rw-r--r-- 1 root           root                682614 Jun 22 10:16
report.xml
     certain-death@my-toshiba:~/recovery/recup_dir.1$
```

By providing root access to the files recovered by Photorec, the secure data recovery process can be realized. Root access ensures that no user other than root can access these files. Users who can access these recovery files are only those who have root access or are granted access by root, where the root is the highest user in the system.

IV. CONCLUSION

Based on the tests that have been carried out, it can be concluded that: 1.) Photorec is a reliable digital forensic tool for data recovery that supports secure data recovery because it can restore all files completely (100%), 2.) Secure data recovery on Photorec implemented in the form of providing root access for all recovered files so that they cannot be accessed by any user without granted access.

V. ACKNOWLEDGMENTS

The authors are grateful to the Indonesia Linux Open Source Community, Udayana University, and family for supporting this research during Covid-19 pandemic in 2020.

REFERENCES

[1] Raptis, et al., Data Management in Industry 4.0: State of the Art and Open Challenges, **IEEE Access, 7,** 2019, pp. 1-43.

[2] I. D. P. G. W. Putra, M. D. W. Aristana, Perancangan Desain Ruangan Data Center Menggunakan Standar TIA-942, ***Jurnal RESISTOR (Rekayasa Sistem Komputer), 2*:1**, 2019, pp.1-5.

[3] B. Raharjo, Sekilas Mengenai Forensic Digital, Jurnal Sosioteknologi, 2013, pp.384-387.

[4] K.P. Chow, S. Shenoi, Advances in Digital Forensics VI, **IFIP AICT 337 International Federation for Information Processing,** 2010, pp. 297–311.

[5] I. Riadi, Sunardi, M.E. Rauli, Identifikasi Bukti Digital WhatsApp pada Sistem Operasi Proprietary Menggunakan Live Forensics, ***Jurnal Teknik Elektro*, 10,** 2018.

[6] A. Fauzan, I. Riadi, A. Fadlil, Analisis Forensik Digital Pada Line Messenger Untuk Penanganan Cybercrime, **Prosiding Annual Research Seminar, 2,** 2016.

[7] G.B. Santoso, D. Dirgantara, Disaster Recovery Plan dalam Kantor Samisami, **Proseding Seminar Nasional Cendekiawan ke 3**, 2017.

[8] B. Yuliadi, A. Nugroho, Rancangan Disaster Recovery Pada Instansi Pendidikan Studi Kasus Universitas Mercu Buana, ***Jurnal Teknik Informatika*, 9,** 2016.

[9] A. Supriyanto, I. Aknuranda, W.H.N. Putra, Penyusunan Disaster Recovery Plan (DRP) berdasarkan Framework NIST SP 800-34 (Studi Kasus: Departemen Teknologi Informasi PT Pupuk Kalimantan Timur), ***Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer, 3:8***, 2019, hlm.8212-8219

[10] A. Yudhana, R. Umar, A. Ahmadi, Digital Evidence Identification on Google Drive in Android Device Using NIST Mobile Forensic Method, ***Scientific Journal of Informatics*****,** 6**,** 2019.

[11] J.B. Wollaston, T. Storer, W. Glisson, Comparison of the Data Recovery Function of Forensic Tools, **IFIP International Federation for Information Processing, 22**, 2013.

[12] O.S. Sitompul, A. Handoko, R.F. Rahmat, File Reconstruction in Digital Forensic, **TELKOMNIKA, 16**, 2018, pp.776~794

[13] A. Bansal, A. Agrawal, M.S. Sankhla, R. Kumar, Computer Forensic Investigation on Hard Drive Data Recovery: A Review Study*,* ***IOSR Journal of Computer Engineering (IOSR-JCE), 18***, 2016, pp.39-42.

[14] I. Lazaridis, T. Arampatzis, S. Pouros, Evaluation of Digital Forensics Tools on Data Recovery and Analysis, **Proceedings of the Third International Conference on Computer Science, Computer Engineering, and Social Media (CSCESM2016)**, Thessaloniki, Greece, 2016.

[15] M. Riskiyadi, Investigasi Forensic Terhadap Bukti Digital Dalam Mengungkap Cybercrime, ***Jurnal Saintek, 3,*** 2020.

[16] H. Handrizal, Analisis Perbandingan Toolkit Puran File Recovery, Glary Undelete Dan Recuva Data Recovery Untuk Digital Forensik, ***Jurnal Komputer dan Sain Informatika (J-SAKTI), 1,*** 2017.

[17] I. Riadi, S. Sunardi, S. Sahiruddin, Perbandingan Tool Forensik Data Recovery Berbasis Android menggunakan Metode NIST, ***Jurnal Teknologi Informasi dan Ilmu Komputer (JTIIK), 7*****,** 2020.