semanTIK, Vol.6, No.2, Jul-Des 2020, pp. 43-50
ISSN: 2502-8928 (Online)
DOI : 10.5281/zenodo.4395793
Terakreditasi "Peringkat 4 (Sinta 4)" oleh Kemenristekdikti
Website : http://ojs.uho.ac.id/index.php/semantik

REVIEW *EASEUS DATA RECOVERY WIZARD* UNTUK DIGITAL FORENSIK

Handrizal
Program Studi S1 Ilmu Komputer Fakultas Ilmu Komputer dan Teknologi Informasi
Universitas Sumatera Utara
e-mail: **Handrizal@usu.ac.id**

Abstrak

Makalah ini menyajikan review sebuah aplikasi yang bernama *EaseUS Data Recovery Wizard* yang digunakan untuk pemulihan data yang sudah dihapus. Penelitian ini dilakukan untuk melihat kemampuan aplikasi ini dalam pemulihan data yang dihapus pada sebuah USB *flash drive* dan menggunakan metode *National Institute of Standard and Technology* (NIST). Hasil dari pengujian menunjukkan bahwa aplikasi ini dapat berkerja dengan baik dalam hal menemukan semua data yang sudah dihapus, akan tetapi kurang handal dalam memulihkan data yang sudah dihapus tersebut. Hasil pengujian terhadap sepuluh data yang hanya empat(40%) data yang berhasil di pulihkan.

Kata kunci: Data, *Recovery*, Forensik, *EaseUS*

Abstract

This paper presents a review of an application called EaseUS Data Recovery Wizard used for recovering deleted data. This research was conducted to see the ability of this application in recovering deleted data on a USB flash drive and using the National Institute of Standard and Technology (NIST) method. The results of testing indicate that this application can work well in terms of finding data that has been deleted but is less reliable in recovering data that has been deleted. Test results on ten data of which only four (40%) data were recovered.

Keywords: *Data, Recovery, Forensic, EaseUS*

1. PENDAHULUAN

Salah satu dampak negatif yang timbulkan dari kemajuan teknologi adalah penyalahgunaan teknologi tersebut untuk kejahatan. Kejahatan yang berkaitan dengan penggunaan komputer pada media tersebut biasanya dikenal dengan nama *cybercrime*. Istilah ini juga digunakan untuk kegiatan kejahatan tradisional di mana komputer atau jaringan komputer digunakan untuk mempermudah atau memungkinkan kejahatan itu terjadi. Contoh kejahatan *cybercrime* di mana komputer sebagai alat adalah spamming dan kejahatan terhadap hak cipta serta kekayaan intelektual. Contoh kejahatan *cybercrime* di mana komputer sebagai sasarannya adalah akses ilegal (mengelabui kontrol akses), *malware* dan serangan DoS. Contoh kejahatan *cybercrime* di mana komputer sebagai tempatnya adalah penipuan identitas. Sedangkan contoh kejahatan tradisional dengan komputer sebagai alatnya adalah pornografi anak dan judi online.

Perilaku *cybercrime* sudah tentu sangat merugikan korbannya dan bertentangan dengan hukum. Untuk memberi hukuman kepada pelaku *cybercrime* ini pihak berwajib biasanya akan mencari beberapa alat bukti. Salah satu alat bukti adalah komputer yang digunakan oleh pelaku. Data yang ada didalam komputer akan diambil sebagai alat bukti dalam menghukum pelaku *cybercrime*. Dalam prakteknya data didalam komputer tersebut

sudah dihapus oleh pelaku sebelum komputer tersebut disita oleh pihak berwajib. Dalam hal inilah diperlukan aplikasi untuk mencari data yang sudah dihapus tersebut. Proses pencarian data yang sudah dihapus ini disebut dengan istilah digital forensik.

1.1 *Data Recovery*

Menurut Juju[1], Data *recovery* adalah proses penyelamatan data yang rusak, tidak bisa diakses, atau terformat dari media penyimpanan. Karena fungsinya adalah untuk menggembalikan data yang hilang maka proses data *recovery* ini bisa digunakan dalam konteks komputer forensik atau untuk mata-mata[2].

1.2. Digital Forensik

Menurut Lazaridis[3], Digital forensik adalah ilmu yang membahas penemuan, validasi dan interpretasi bukti digital yang ditemukan pada perangkat elektronik yang sesuai dengan kejatahan komputer. Sedangkan menurut Sulianta[4], Digital forensik adalah pengaplikasian ilmu pengetahuan dalam mengidentifikasi, mengumpulkan, menguji, dan menganalisis data, kemudian menghadirkan informasi yang dapat diandalkan[5].

1.3 *EaseUS Data Recovery Wizard*

EaseUS Data Recovery Wizard merupakan *software recovery* file gratis untuk sistem operasi Windows dan Mac yang digunakan untuk memulihkan *file* yang dihapus oleh pengguna dari hard drive internal dan ekternal, serta perangkat USB, kartu memori, pemutar musik dan perangkat sejenisnya[6].

2. METODE PENELITIAN

Metodologi yang digunakan untuk penelitian ini adalah *National Institute of Standard and Technology* (NIST) yang dibagi menjadi empat tahap yakni, *Collection*, *Examination*, *Analysis*, dan *Reporting*[7], Masing-masing fase yang berbeda ini dijelaskan lebih lanjut:

a) *Collection*
Collection merupakan proses identifikasi barang bukti yang digunakan berupa perangkat keras yang akan diambil datanya untuk digunakan sebagai bukti digital. Pada penelitian ini penulis menggunakan sebuah perangkat keras *flash disk* Kingston 512 MB.

b) *Examination*
Examination merupakan proses pengambilan data pada barang bukti menggunakan *tool* forensik. Pada penelitian ini penulis menggunakan tool forensik *Easeus Data Recovery Wizard*

c) *Analysis*
Tahap ini adalah proses menganalisis dan mengevaluasi kembali data yang ditemukan dari hasil *examination*.

d) *Reporting*
Tahap *reporting* merupakan proses pelaporan hasil analisis dari data yang ditemukan.

2.1 Data yang digunakan

Dalam penelitian ini penulis menggunakan data milik penulis sendiri, data tersebut terdiri *file* umum (pdf, docx, ppt dan lain-lain), seperti terlihat pada Tabel 1.

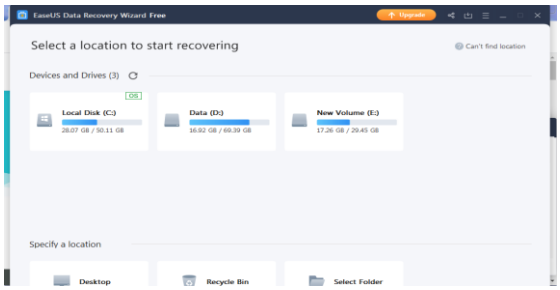
Tabel 1. Data yang digunakan

No.	Nama File	Ekstensi File	Ukuran File (kb)
1.	abc	.docx	13
2.	abcd	.doc	22
3.	abcde	.pdf	81
4.	abcdef	.html	21
5.	abcdefg	.xml	47
6.	abcdefgh	.pptx	34
7.	abcdefghi	.ppt	100
8.	abcdefghij	.xls	9
9.	abcdefghijk	.xps	87
10.	abcdefghijkl	.txt	1

3. HASIL DAN PEMBAHASAN

3.1. Implementasi

Penerapan aplikasi *EaseUS Data Recovery Wizard* dilakukan pada sistem operasi Windows 7. Aplikasi ini adalah software yang bisa di download secara gratis. Setelah *software* tersebut di download kemudian diinstall, tampilan awal untuk aplikasi *EaseUS Data Recovery Wizard* seperti pada Gambar 1.



Gambar 1. Tampilan *EaseUS Data Recovery Wizard*

3.2. Pengujian

Pengujian aplikasi ini dilakukan untuk mengetahui bagaimana kinerja aplikasi dalam pencarian data yang sudah dihapus didalam sebuah *flash drive*. Dalam pengujian ini akan dilihat hasilnya berdasarkan banyaknya jumlah data yang dapat discan dan jumlah data yang dapat dipulihkan.

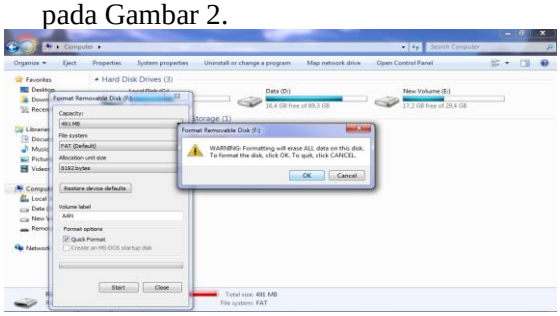
3.3. Pengujian *EaseUS Data Recovery Wizard*

Untuk pengujian dengan *EaseUS Data Recovery Wizard* dilakukan dengan *National Institute of Standard and Technology* (NIST)

3.3.1 *Collection*

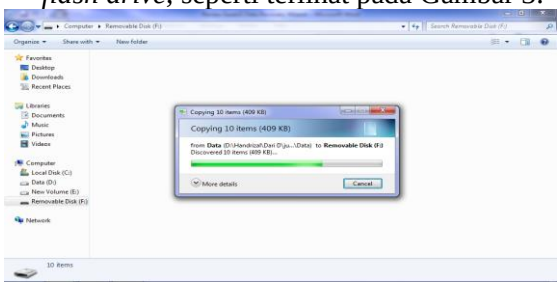
Pada tahap ini dilakukan dengan langkah-langkah berikut ini:

1. Masukkan *USB flash drive* ke port USB.
2. Format *USB flash drive*, seperti terlihat pada Gambar 2.



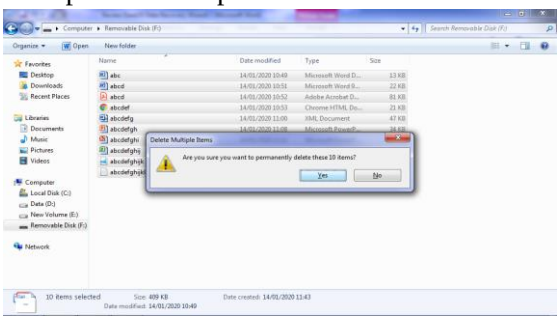
Gambar 2. Format USB flash drive

3. *Copy* sepuluh buah *file* dari *drive* D ke *flash drive*, seperti terlihat pada Gambar 3.



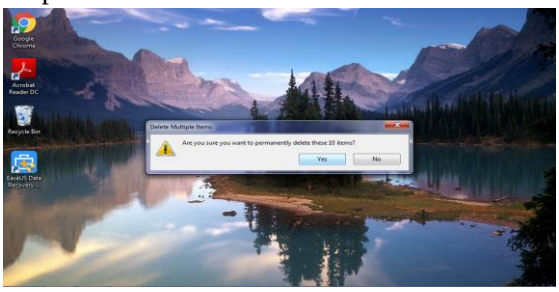
Gambar 3. Proses mengcopy file

4. Hapus semua data didalam *flash drive*, seperti terlihat pada Gambar 4.



Gambar 4. Proses menghapus semua file

5. Kosongkan *recycle bin*, seperti terlihat pada Gambar 5.

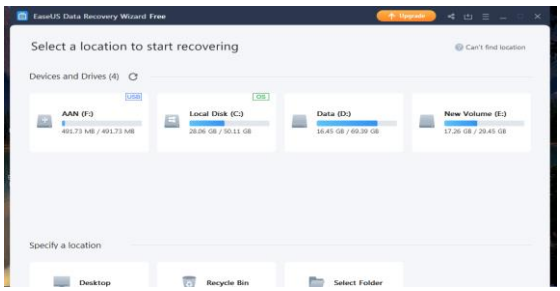


Gambar 5. Proses penghapus *recycle bin*

3.3.2 *Examination*

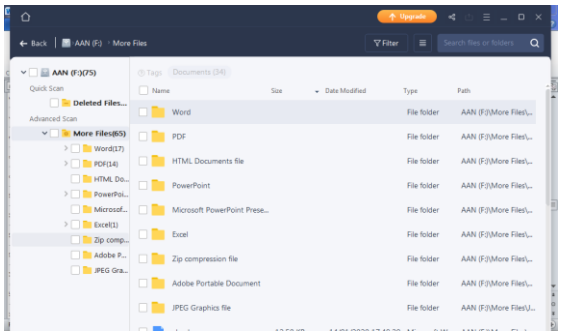
Pada tahap ini dilakukan dengan langkah-langkah berikut ini:

1. Jalankan aplikasi *EaseUS Data Recovery Wizard*. Pada langkah ini akan didapatkan tampilan pada layar aplikasi seperti Gambar 6.



Gambar 6. Proses *scanning* semua *drive*

2. Untuk memilih drive tertentu, klik pada drive yang di inginkan, dalam uji coba ini di pilih drive dengan nama AAN(F), kemudian akan tampil seperti Gambar 7.



Gambar 7. Tampilan proses scan drive F

3. Setelah proses *scan drive* selasai akan tampil seperti Gambar 8.

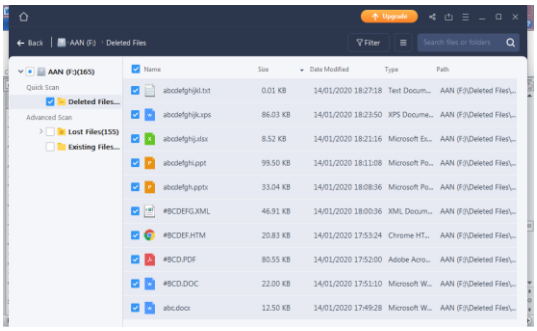
Gambar 8. Hasil proses scan drive

4. Pada gambar 8 terdapat tiga buah *folder* yaitu
   - *Delete Files*
   - *Lost Files*
   - *Existing Files*

5. Untuk memilih *folder* tertentu, klik pada *folder* yang di inginkan, dalam uji coba ini di pilih *folder* dengan nama Delete Files, kemudian akan tampil seperti Gambar 9.

Gambar 9. Tampilan isi *folder Delete Files*

6. Langkah selanjutnya beri tanda *ceklist* pada *file* yang akan di*recovery*, seperti pada Gambar 10.



Gambar 10. Pemilihan *file* yang akan di*recovery*

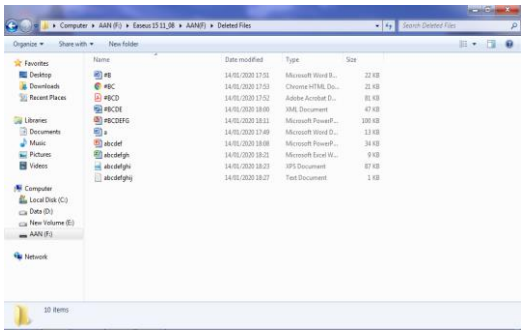
7. Langkah selanjutnya klik "*Recovery*" dan tentukan tempat penyimpan *file* yang akan di*recovery*, seperti pada Gambar 11.

Gambar 11. Proses *recovery file*

8. Setelah proses *recovery* selesai akan tampil seperti Gambar 12.

Gambar 12. Proses *recovery* selesai

9. Setelah proses *recovery* selesai, langkah selanjutnya melihat *file* tersebut pada USB *flash drive*, seperti pada Gambar 13.

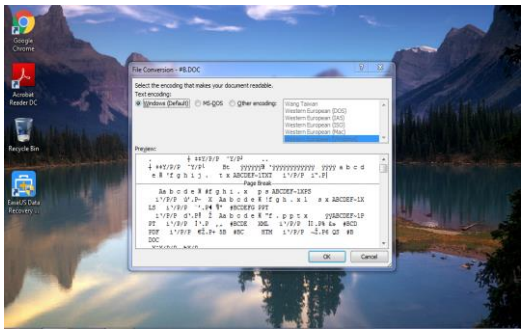


Gambar 13. *File* hasil *recovery*

3.3.3 *Analysis*

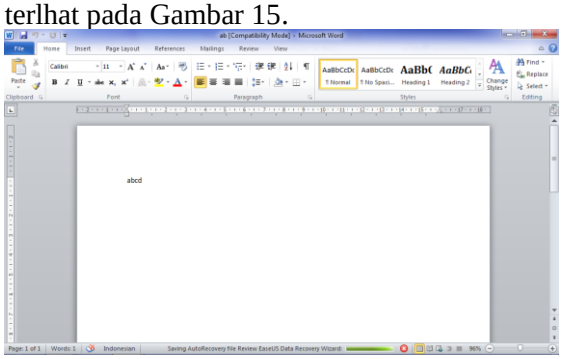
Pada tahap ini dilakukan dengan langkah-langkah berikut ini:

1. Langkah selanjutnya melihat masing-masing isi *file* tersebut pada USB *flash drive*, dalam penelitian ini di coba melhat isi *file* yang pertama seperti pada Gambar 14.



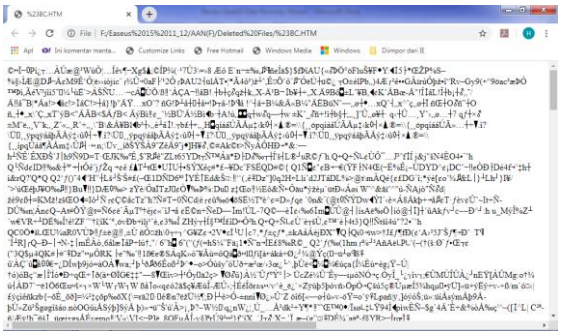
Gambar 14. Isi *file* hasil *recovery*

Pada Gambar 14 dapat dilihat bahwa *file* tersebut tidak bisa dibuka dan hasilnya tidak sesuai dengan isi *file* aslinya seperti terlhat pada Gambar 15.



Gambar 15. Isi *file* hasil sebelum di *delete*

2. Langkah selanjutnya melihat isi *file* yang kedua seperti pada Gambar 16.

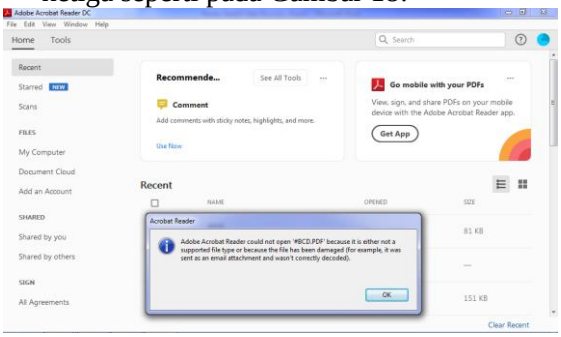


Gambar 16. Isi *file* hasil *recovery*

Pada Gambar 16 dapat dilihat bahwa *file* tersebut tidak bisa dibuka dan hasilnya tidak sesuai dengan isi *file* aslinya seperti terlhat pada Gambar 17.

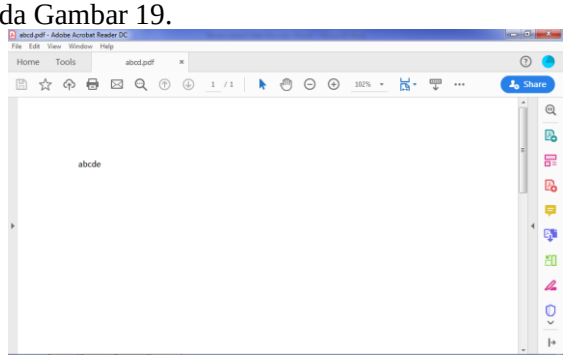
Gambar 17. Isi *file* hasil sebelum di *delete*

3. Langkah selanjutnya melihat isi *file* yang ketiga seperti pada Gambar 18.



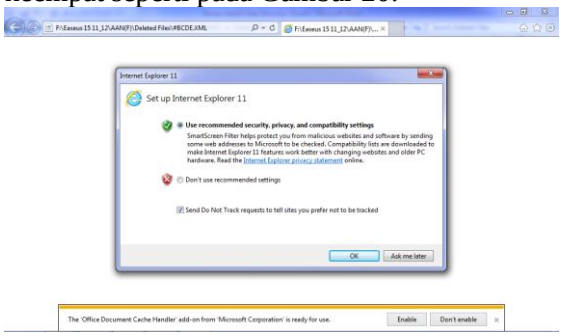
Gambar 18. Isi *file* hasil *recovery*

Pada Gambar 18 dapat dilihat bahwa *file* tersebut tidak bisa dibuka dan hasilnya tidak sesuai dengan isi *file* aslinya seperti terlhat pada Gambar 19.



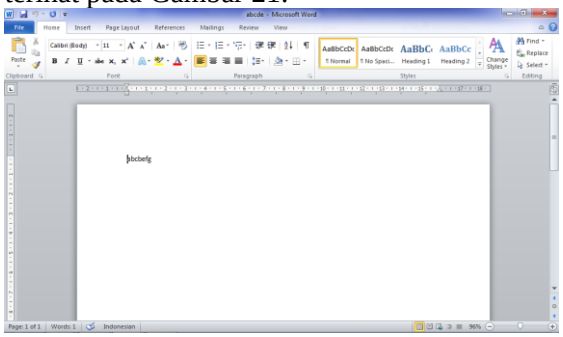
Gambar 19. Isi *file* hasil sebelum di *delete*

4. Langkah selanjutnya melihat isi *file* yang keempat seperti pada Gambar 20.



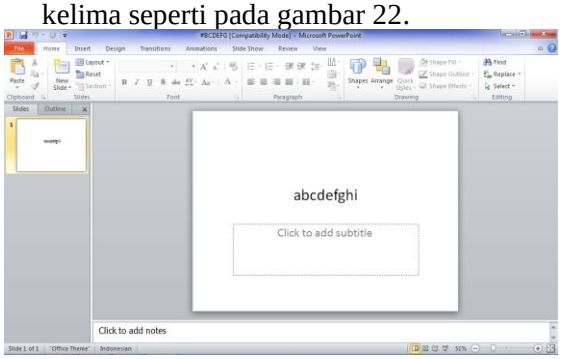
Gambar 20. Isi *file* hasil *recovery*

Pada Gambar 20 dapat dilihat bahwa *file* tersebut tidak bisa dibuka dan hasilnya tidak sesuai dengan isi *file* aslinya seperti terlhat pada Gambar 21.



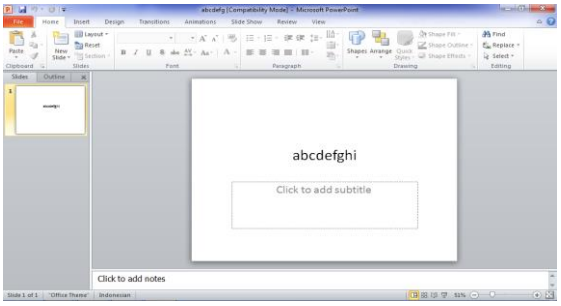
Gambar 21. Isi *file* hasil sebelum di *delete*

5. Langkah selanjutnya melihat isi *file* yang kelima seperti pada gambar 22.



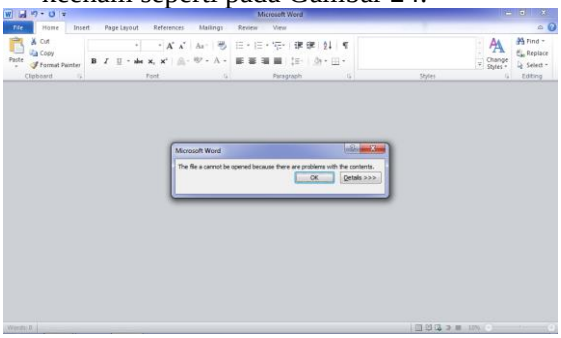
Gambar 22. Isi *file* hasil *recovery*

Pada Gambar 22 dapat dilihat bahwa *file* tersebut bisa dibuka dan hasilnya sama dengan isi *file* aslinya seperti terlhat pada Gambar 23.



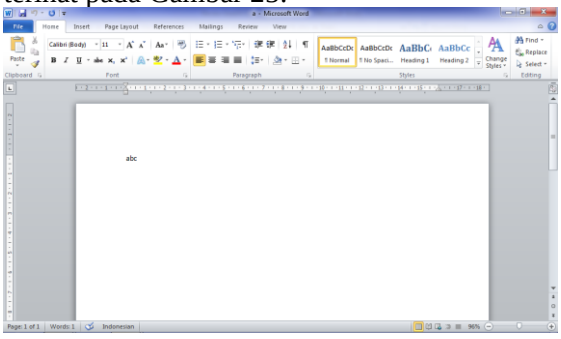
Gambar 23. Isi *file* hasil sebelum di *delete*

6. Langkah selanjutnya melihat isi *file* yang keenam seperti pada Gambar 24.



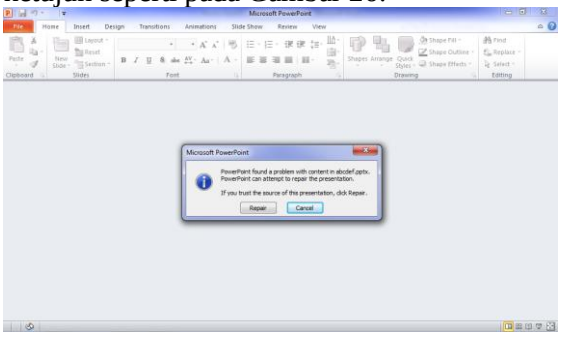
Gambar 24. Isi *file* hasil *recovery*

Pada Gambar 24 dapat dilihat bahwa *file* tersebut tidak bisa dibuka dan hasilnya tidak sesuai dengan isi *file* aslinya seperti terlhat pada Gambar 25.



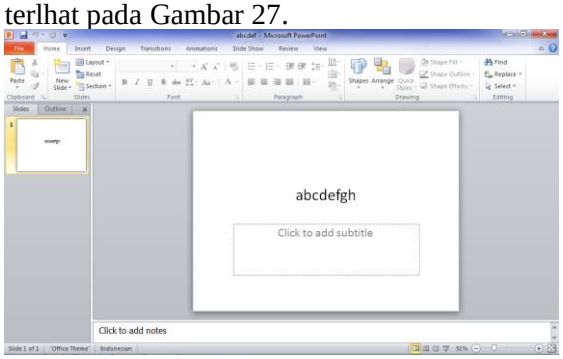
Gambar 25. Isi *file* hasil sebelum di *delete*

7. Langkah selanjutnya melihat isi *file* yang ketujuh seperti pada Gambar 26.



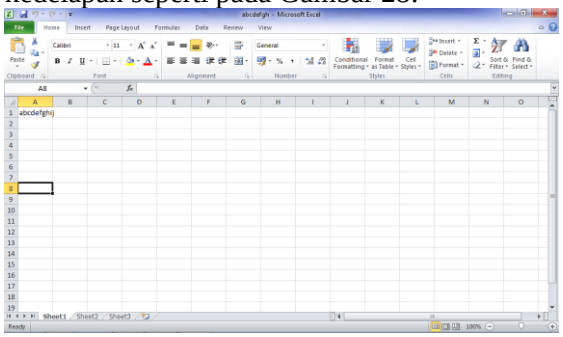
Gambar 26. Isi *file* hasil *recovery*

Pada Gambar 26 dapat dilihat bahwa *file* tersebut tidak bisa dibuka dan hasilnya tidak sesuai dengan isi *file* aslinya seperti terlhat pada Gambar 27.



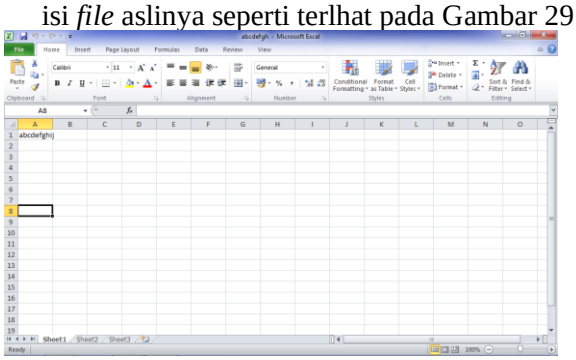
Gambar 27. Isi *file* hasil sebelum di *delete*

8. Langkah selanjutnya melihat isi *file* yang kedelapan seperti pada Gambar 28.



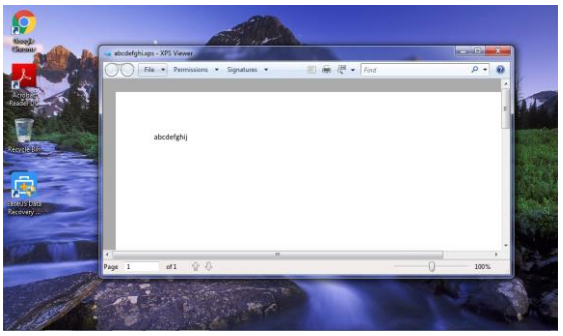
Gambar 28. Isi *file* hasil *recovery*

Pada Gambar 28 dapat dilihat bahwa *file* tersebut bisa dibuka dan hasilnya sam dengan isi *file* aslinya seperti terlhat pada Gambar 29.



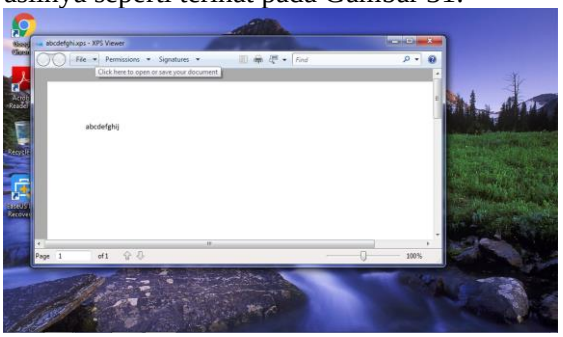
Gambar 29. Isi *file* hasil sebelum di *delete*

9. Langkah selanjutnya melihat isi *file* yang kesembilan seperti pada Gambar 30.



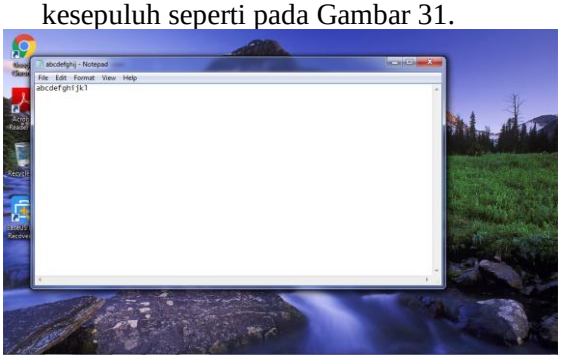
Gambar 30. Isi *file* hasil *recovery*

Pada Gambar 30 dapat dilihat bahwa *file* tersebut bisa dibuka dan hasilnya sama dengan isi *file* aslinya seperti terlhat pada Gambar 31.



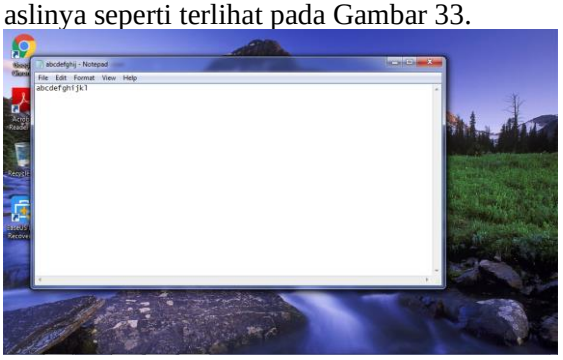
Gambar 31. Isi *file* hasil sebelum di *delete*

10. Langkah selanjutnya melihat isi *file* yang kesepuluh seperti pada Gambar 31.



Gambar 32. Isi *file* hasil *recovery*

Pada Gambar 32 dapat dilihat bahwa *file* tersebut bisa dibuka dan hasilnya sama dengan isi *file* aslinya seperti terlihat pada Gambar 33.



Gambar 33. Isi *file* hasil sebelum di *delete*

3.3.4 *Reporting*

Dari pengujian yang sudah dilakukan menggunakan USB flash drive, diperoleh hasil seperti terlihat pada Tabel 2.

Tabel 2. Hasil Pengujian *EaseUS Data Recovery Wizard*

No	Parameter	Hasil
1	Jumlah data yang berhasil di *scan*	10
2	Jumlah data yang berhasil di *recovery*	4

Berdasarkan Tabel 2 diketahui bahwa aplikasi *EaseUS Data Recovery Wizard* yang digunakan dapat menemukan semua file yang sudah dihapus, tetapi hanya mampu memulihkan kembali 4 *file* (40%) yang sudah dihapus tersebut, hal ini kemungkinan terjadi karena perangkat *flash disk* yang digunakan sudah diformat dan data pada *recycle bin* juga dikosongkan, sehingga datanya menjadi susah untuk dipulihkan.

4. KESIMPULAN

Berdasarkan penelitian yang telah dilakukan dapat ambil kesimpulan, antara lain:

1. Aplikasi *EaseUS Data Recovery Wizard* dapat menemukan semua file yang sudah dihapus dalam sebuah *flash drive* dan sudah dikosong dari *recycle bin.*
2. Aplikasi *EaseUS Data Recovery Wizard* hanya dapat memulihkan 4 file (40%) yang sudah dihapus dalam sebuah *flash drive*.

5. SARAN

1. Untuk mengetahui lebih jauh mengenai kemampuan aplikasi ini, disarankan untuk melakukan pengujian terhadap media penyimpan yang lain.
2. Selain aplikasi yang sudah diuji dalam penelitian ini, masih banyak aplikasi yang lainnya. Untuk itu disarankan agar melakukan penelitian dengan menggunakan aplikasi yang lain.

DAFTAR PUSTAKA

[1] D. Juju, "*Data Recovery, Pulihkan Data dengan Tool Sederhana dan Mudah*." Elex Media Komputindo, 2008.

[2] B. Mathew, "*File Data Recovery : PC Hard drive Data Recovery, USB Data Recovery, Mac Data Recovery, Android Data Recovery, Data Recovery Services"*. CreateSpace Independent Publishing Platform, 2014.

[3] I. Lazaridis, T. Arampatzis, and S. Pouros, "*Evaluation of Digital Forensics Tools on Data Recovery and Analysis*," *Third Int. Conf. Comput. Sci. Comput. Eng. Soc. Media*, pp. 67–71, 2016.

[4] F. Sulianta, "*Komputer Forensik*." PT Elex Media Komputindo, Jakarta, 2008.

[5] V. Singh, A. Tarannum, and V. Saran, "*Efficiency of open source tools for Recovery of Unconventional deleted data : A Review*," no. August, pp. 19–24, 2015.

[6] T. Fisher, "*A Full Review of EaseUS Data Recovery Wizard a free file undelete tool*." 2020, [Online]. Available: https://www.lifewire.com/easeus-data-recovery-wizard-review-2622879.

[7] I. Riadi, S. 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.