semanTIK, Vol.4, No.2, Jul-Des 2018, pp. 21-28
ISSN: 2502-8928 (Online)
DOI : 10.5281/zenodo.1438737

ANALISIS PERBANDINGAN *TOOLKIT* RECUVA DATA *RECOVERY* DAN STELLAR PHOENIX WINDOWS DATA *RECOVERY* UNTUK DIGITAL FORENSIK

Handrizal
Program Studi D3 Manajemen Informatika
AMIK Tunas Bangsa Pematangsiantar
Jl. Jend. Sudirman Blok I No. 1, 2, & 3 Pematangsiantar
e-mail : **handrizal_tanjung@yahoo.com**

Abstrak

Penelitian ini menyajikan analisa perbandingan dua *toolkit* digital forensik untuk skenario pemulihan data yang sudah dihapus. *Toolkit* yang digunakan adalah Recuva Data *Recovery* dan Stellar Phoenix Windows Data *Recovery*. Kemampuan mereka dalam pemulihan data yang dihapus telah diuji dan dianalisa dalam sebuah USB *flash drive*. Hasil dari perbandingan menunjukkan bahwa kedua *toolkit* ini dapat berkerja dengan baik dalam hal menemukan data yang sudah dihapus maupun dalam memulihkan data yang sudah dihapus tersebut.

Kata Kunci—Data, *Recovery*, Forensik, Recuva, Stellar

Abstract

This paper presents an analysis with two digital forensic toolkits for deleted data scenarios. The used toolkit is Recuva Data Recovery and Stellar Phoenix Windows Data Recovery. They can recover data that is being and analyzed in a USB flash drive. The results of the comparison that the two toolkits can work well regarding finding data that has been discarded or in recovering the deleted data.

Keywords*—Data, Recovery, Forensic, Recuva, Stellar*

1. PENDAHULUAN

Kemajuan dibidang teknologi seperti media massa, *game* online dan media sosial seperti facebook, twitter, instagram telah menjangkiti kehidupan dalam bermasyarakat, khususnya generasi muda. Salah satu dampak negatif yang ditimbulkan dari kemajuan teknologi ini adalah penyalahgunaan teknologi tersebut untuk kejahatan. Kejahatan yang berkaitan dengan penggunaan komputer pada media tersebut biasanya dikenal dengan nama *cybercrime*.

Walaupun kejahatan *cybercrime* umumnya mengacu kepada aktivitas kejahatan dengan komputer atau jaringan komputer sebagai unsur utamanya, istilah ini juga digunakan untuk kegiatan kejahatan tradisional dimana komputer atau jaringan komputer digunakan untuk mempermudah atau memungkinkan kejahatan itu terjadi. Contoh kejahatan *cybercrime* dimana komputer sebagai alat adalah *spamming* dan kejahatan terhadap hak cipta dan kekayaan intelektual. Contoh kejahatan *cybercrime* dimana komputer sebagai sasarannya adalah akses ilegal (mengelabui kontrol akses), malware dan serangan DoS. Contoh kejahatan *cybercrime* dimana 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 di

dalam komputer akan diambil sebagai alat bukti dalam menghukum pelaku *cybercrime*. Dalam prakteknya data di dalam komputer tersebut sudah dihapus oleh pelaku sebelum komputer tersebut disita oleh pihak berwajib. Dalam hal inilah diperlukan *toolkit* untuk memulihkan data yang sudah dihapus tersebut.

2.METODE PENELITIAN

2.1. Data Recovery

Menurut [1], data *recovery* adalah proses pengembalian data dari kondisi yang rusak, gagal, korup atau tidak bisa diakses ke kondisi awal yang normal. Data yang dikembalikan bisa dari *hardisk*, *flash disk* dan media simpan lainnya seperti camera digital dan *camcorder*. Karena fungsinya adalah untuk menggembalikan data yang hilang maka proses data *recovery* ini bisa digunakan dalam konteks komputer forensik atau untuk mata-mata [2].

2.2. Digital Forensik

Menurut [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 [4], digital forensik adalah pengaplikasian ilmu pengetahuan dalam mengidentifikasi, mengumpulkan, menguji dan menganalisa data, kemudian menghadirkan informasi yang dapat diandalkan.

2.3. Recuva Data Recovery

Recuva merupakan *software recovery file* penting yang digunakan untuk memulihkan *file* yang dihapus oleh pengguna dari PC Windows, *recycle bin* atau dari MP3 *player* [4]. Menurut [5], recuva merupakan *software* yang bekerja secara terpadu untuk memulihkan semua data, *file*, photo hanya dengan satu kali klik.

2.4. Stellar Phoenix Windows Data Recovery

Stellar Phoenix Windows Data *Recovery* merupakan *software* utilitas yang dapat mengembalikan *file* atau data yang hilang pada media penyimpanan seperti USB *flash disk* maupun *hardisk* [6]. Kehilangan data ini biasanya di sebabkan oleh banyak hal seperti kesalahan sewaktu melakukan format *hardisk*, terinfeksi virus, maupun karena disebabkan oleh program yang tidak berjalan dengan benar [4].

2.5. Metodologi Penelitian

Metodologi yang digunakan untuk penelitian ini dibagi menjadi empat tahap yaitu tahap format media penyimpanan, tahap pengisian media penyimpanan, tahap penghapusan data dan tahap pemulihan dengan perangkat lunak. Masing-masing fase yang berbeda ini dijelaskan sebagai berikut :

1. Format Media Penyimpanan

Format digunakan untuk menghapus informasi yang ada pada sebuah media penyimpanan seperti *hardisk*, disket, *flash disk* dan lain-lain. Dalam penelitian ini media penyimpan terlebih dahulu diformat untuk memastikan bahwa media tersebut dalam kondisi bersih sebelum dipergunakan untuk menyimpan data.

2. Pengisian Media Penyimpanan

Media penyimpanan yang sudah diformat sudah bisa dipergunakan untuk menyimpan data, dalam penelitian ini penulis menggunakan *flash disk* untuk media penyimpanan. *Flash disk* yang sudah diformat akan diisi dengan beberapa *file* yang sudah di dalam sebuah *hardisk*.

3. Penghapuskan Data

Secara umum, menghapus mengacu pada tindakan menghilangkan *file*, teks atau objek lain dari *hard drive* komputer atau media lainnya. Misalnya, jika memiliki gambar di komputer yang tidak lagi diinginkan, itu bisa dihapus.

File yang dihapus di Microsoft Windows dikirim ke *Recycle bin*. Di sebagian besar sistem operasi, ketika *file* dihapus, mereka hanya ditandai seperti itu, tetapi masih ada di *hard drive* sampai mereka ditimpa oleh data lain. Kondisi inilah yang memungkinkan pemulihan data. Dalam penelitian ini penulis juga akan menghapus *file* yang berada di dalam *Recycle bin* akan ikut dihapus, untuk memastikan bahwa *file* tersebut sudah tidak ada di dalam media bersangkutan. Metode yang secara konvensional digunakan untuk penghapusan *file* atau data digital dari informasi berharga terdiri dari menekan

tombol “Del” atau menggunakan kombinasi “Shift + Del “.

4. Pemulihan dengan Perangkat Lunak

Tahapan ini adalah yang paling penting, dalam tahap ini akan dilakukan percobaan pemulihan data yang sudah dihapus dengan menggunakan dua buah *toolkit* yaitu, Recuva Data *Recovery* dan Stellar Phoenix Windows Data *Recovery*. Hasil dari kedua *toolkit* ini akan dianalisa untuk melihat perbandingannya.

2.6. Perangkat yang Digunakan

Dalam penelitian ini perangkat yang digunakan terdiri dari dua jenis, yaitu:

a. Perangkat Keras
   1. Notebook
      Prosessor : Intel Atom N 450
      RAM : 1 GB
      Tipe Sistem : 32-Bit
   2. *Hardisk*
      Hitachi 160 GB
   3. *Flash disk*
      Kingston 512 MB

b. Perangkat Lunak
   1. Sistem Operasi
      Windows 7 Professional
   2. Perangkat Lunak *Recovery*
      a. RecuvaData *Recovery* Ver. 1.53.1087
      b. Stellar Phoenix Windows Data *Recovery* Ver. 7.0.0.3

2.7 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.

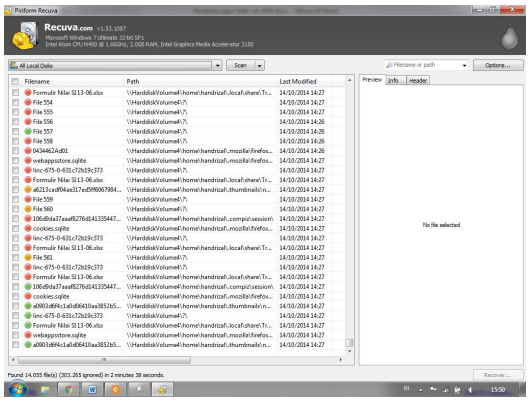
Tabel 1 Data yang Digunakan

No.	Nama *File*	Ekstensi *File*	Ukuran *File* (Kb)
1.	A	.docx	13
2.	B	.pptx	32
3.	C	.pdf	78
4.	D	.xlsx	9
5.	E	.xml	47
6.	F	.doc	22
7.	G	.ppt	100
8.	H	.xls	23
9.	I	.rtf	32
10.	J	.html	1

3. HASIL DAN PEMBAHASAN

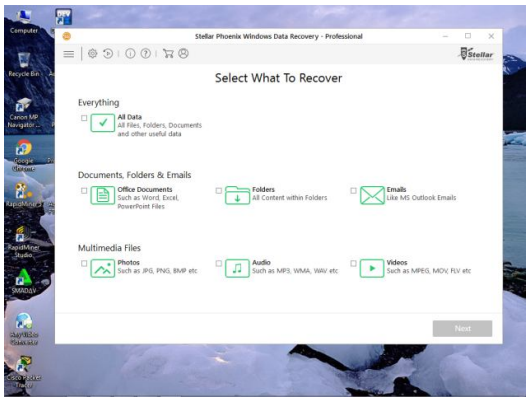
3.1. Implementasi

Penerapan *toolkit* Recuva Data *Recovery* dan Stellar Phoenix Windows Data *Recovery*, dilakukan pada sistem operasi windows 7. Kedua *toolkit* ini adalah *software* yang bisa di-*download* secara gratis. Setelah kedua *software* tersebut di-*download* kemudian di-*install*. Tampilan awal untuk *toolkit* Recuva Data *Recovery* seperti pada Gambar 1.



Gambar 1. Tampilan Recuva Data Recover

Sedangkan tampilan awal untuk Stellar Phoenix Windows Data *Recovery* seperti terlihat pada Gambar 2.



Gambar 2. Tampilan awal Stellar Phoenix Windows Data *Recovery*.

3.2. Pengujian

Pengujian kedua *toolkit* ini dilakukan untuk mengetahui bagaimana kinerja *toolkit* dalam pencarian data yang sudah dihapus di dalam sebuah *flash drive*. Dalam pengujian ini akan dilihat hasilnya berdasarkan banyaknya jumlah data yang dapat di-*scan* dan jumlah data yang dapat dipulihkan. Tahap pertama pengujian akan dilakukan dengan

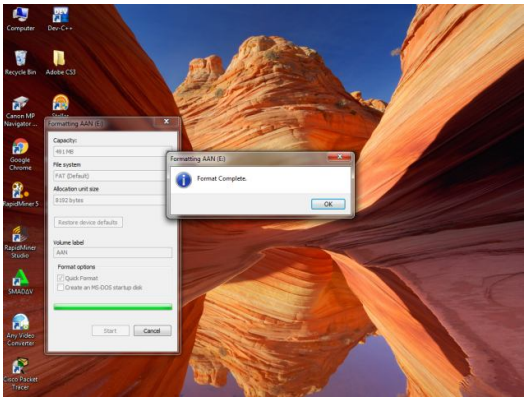
menggunakan *toolkit* Recuva Data *Recovery*. Kemudian pengujian dilanjutkan dengan *toolkit* Stellar Phoenix Windows Data *Recovery*. Tahap-tahap pengujian untuk masing-masing *toolkit* seperti berikut:

a. Memformat *flash drive*.
b. Meng-*copy* sepuluh buah *file* dari *drive* D ke *flash drive*.
c. Menghapus semua data di dalam *flash drive*.
d. Mengosongkan *recycle bin*.
e. Mengoperasikan *toolkit*

3.3. Pengujian Recuva Data *Recovery*

Untuk pengujian dengan Recuva Data *Recovery* dilakukan dengan langkah-langkah berikut ini:

1. Memasukkan USB *flash drive* ke port USB.
2. Memformat USB *flash drive*, seperti terlihat pada Gambar 3.

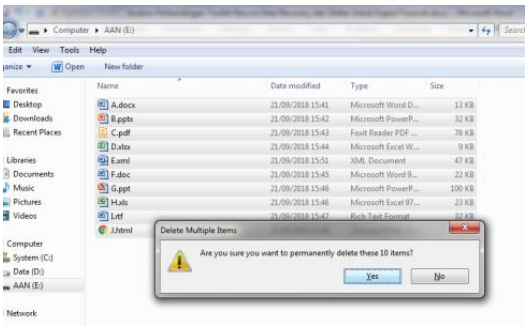


Gambar 3. Memformat USB *Flash Drive*

3. Meng-*copy* sepuluh buah *file* dari *drive* D ke *flash drive*, seperti terlihat pada Gambar 4.

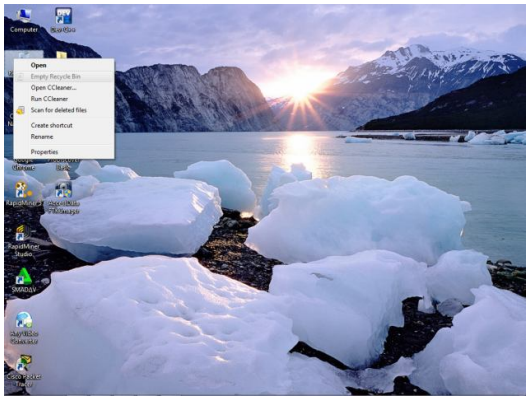
Gambar 4. Proses Meng-*copy File*

4. Menghapus semua data di dalam *flash drive*, seperti terlihat pada Gambar 5.



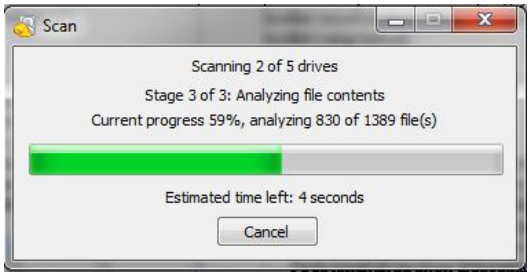
Gambar 5. Proses Menghapus Semua *File*

5. Mengosongkan *recycle bin*, seperti terlihat pada Gambar 6.



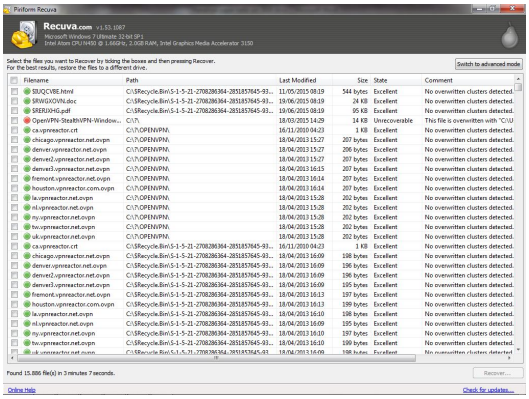
Gambar 6. Proses Menghapus *Recycle Bin*

6. Menjalankan Aplikasi Recuva Data *Recovery*. Pada langkah ini akan didapatkan tampilan pada layar aplikasi seperti Gambar 7.

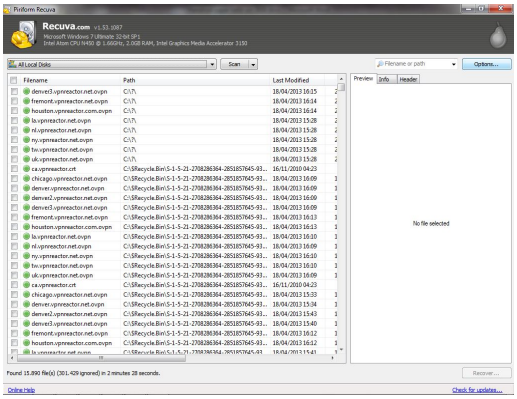


Gambar 7. Proses *Scanning* Semua *Drive*

7. Setelah proses *scanning* semua *drive* selesai, akan tampil hasil *scanning* semua *drive* tersebut seperti terlihat pada Gambar 8.
8. Untuk memilih *drive* tertentu, klik pada bagian " *Switch to advanced mode*", kemudian akan tampil seperti Gambar 9.

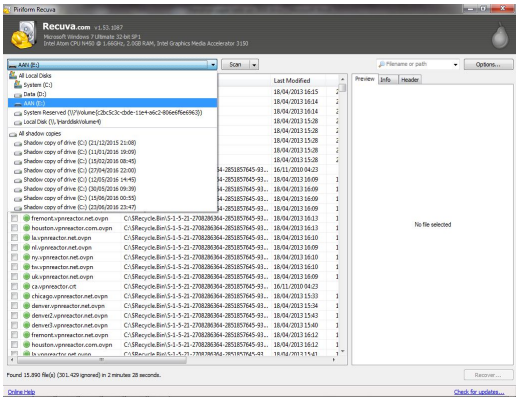


Gambar 8. Hasil *Scanning* Semua *Drive*



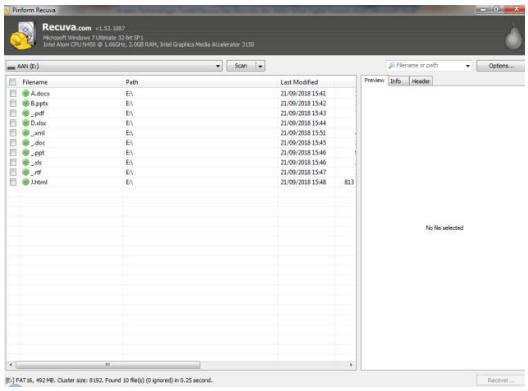
Gambar 9. Tampilan *Mode Advanced*

9. Meng-klik pada tulisan '*All local disks*", kemudian pilih USB *flash drive*. Pada proses ini akan tampil seperti Gambar 10.



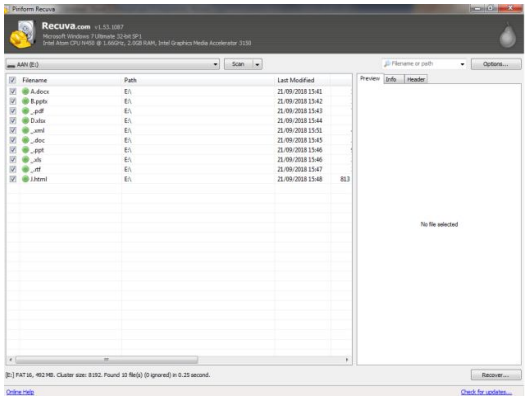
Gambar 10. Proses Pemilihan *Drive*

10. Kemudian setelah *drive* USB *flash* dipilih, langkah selanjutknya klik "*scan*". Proses ini akan tampil seperti Gambar 11.



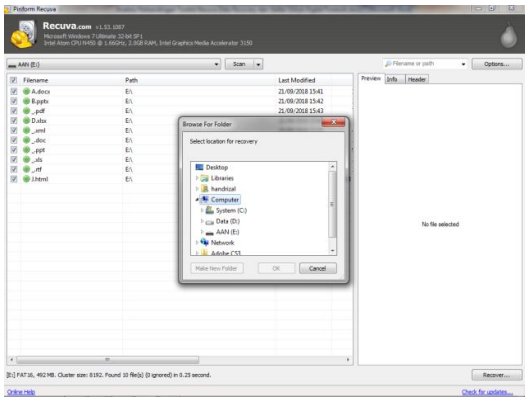
Gambar 11. Proses *Scanning* USB *Flash Drive*

11. Langkah selanjutnya memberi tanda ceklist pada *file* yang akan di-*recovery*, seperti pada Gambar 12.



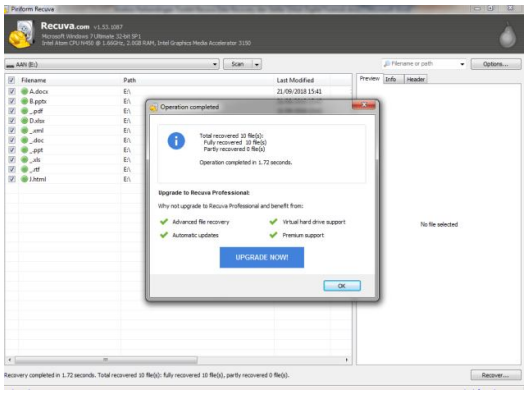
Gambar 12. Pemilihan *File* yang Akan Di-*recovery*

12. Langkah selanjutnya klik "*Recovery*" dan tentukan tempat penyimpan *file* yang akan di-*recovery*, seperti pada Gambar 13.



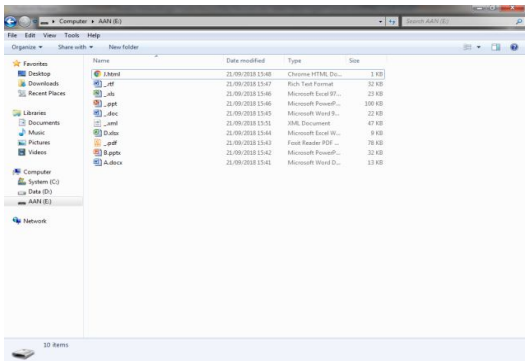
Gambar 13. Proses *Recovery File*

13. Setelah proses *recovery* selesai akan tampil seperti Gambar 14.



Gambar 14. Proses *Recovery* Selesai

14. Setelah proses *recovery* selesai, langkah selanjutnya melihat *file* tersebut pada USB *flash drive*, seperti pada Gambar 15.

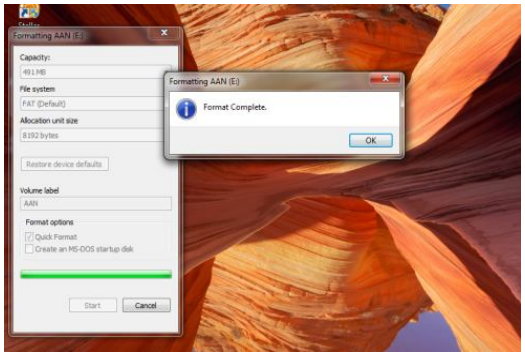


Gambar 15. *File* Hasil *Recovery*

3.4. Pengujian Stellar Phoenix Windows Data *Recovery*

Pada pengujian dengan Puran *file recovery* dilakukan dengan langkah-langkah berikut ini:

1. Memasukkan USB *flash drive* ke port USB.
2. Memformat USB *flash drive*, seperti terlihat pada Gambar 16.

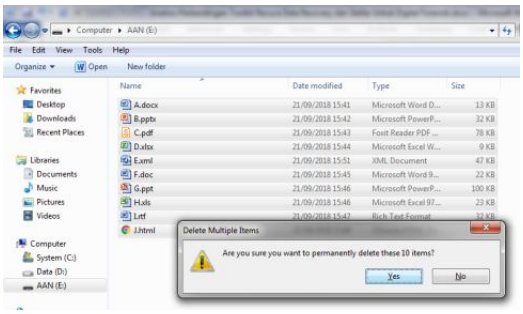


Gambar 16. Memformat USB *Flash Drive*

3. Meng-*copy* sepuluh buah *file* dari *drive* D ke *flash drive*, seperti terlihat pada Gambar 17.

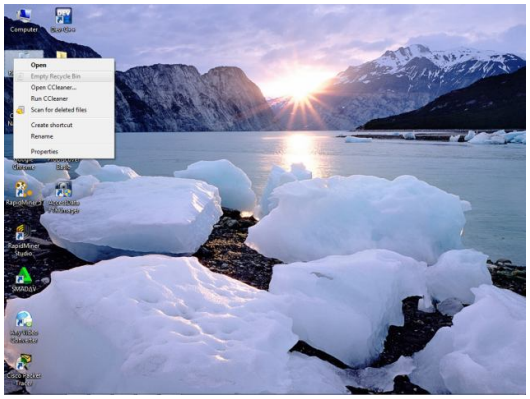
Gambar 17. Proses Meng-*copy File*

4. Menghapus semua data di dalam *flash drive*, seperti terlihat pada Gambar 18.



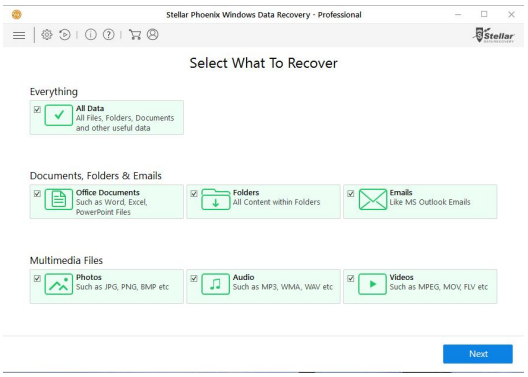
Gambar 18. Proses Menghapus Semua *File*

5. Mengkosongkan *recycle bin*, seperti terlihat pada Gambar 19.



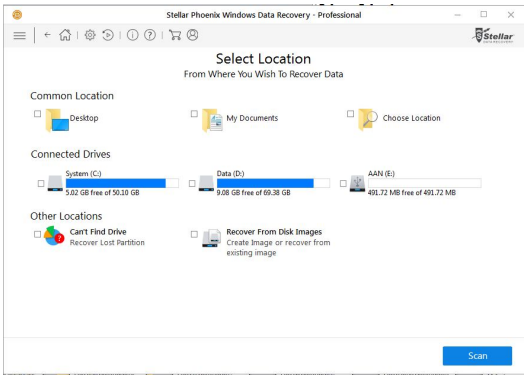
Gambar 19. Proses Menghapus *Recycle Bin*

6. Menjalankan aplikasi Stellar Phoenix Windows Data *Recovery*. Pada langkah ini akan didapatkan tampilan pada layar aplikasi seperti Gambar 20.



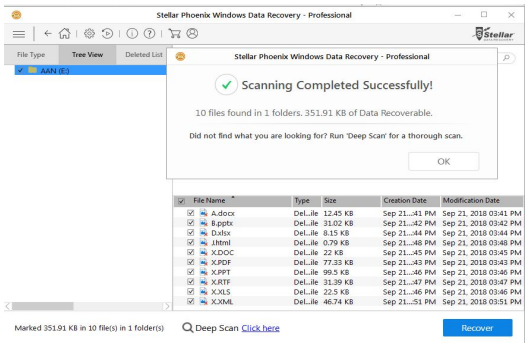
Gambar 20. Tampilan Awal Stellar Phoenix Windows Data *Recovery*

7. Langkah selanjutnya klik "Next" akan tampil seperti Gambar 21.



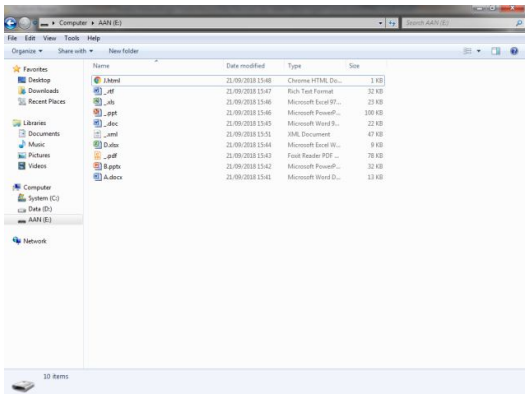
Gambar 21. Tampilan Pilihan Lokasi yang Akan Di-*recovery*

8. Langkah selanjutnya memberi tanda ceklist pada USB *flash drive* yang akan di-*recovery* kemudian klik "*Scan*", seperti pada Gambar 22.



Gambar 22. Akhir Proses *Scan* USB *flash drive*

9. Langkah selanjutnya klik "*Recovery*". Setelah proses *recovery* selesai, langkah selanjutnya melihat *file* tersebut pada USB *flash drive*, seperti pada Gambar 23 .



Gambar 23. *File* Hasil *Recovery*

3.5. HasilPengujian

Dari pengujian yang sudah dilakukan menggunakan USB *flash drive* seperti yang telah disebutkan, diperoleh hasil seperti terlihat pada Table 2.

Tabel 2. Perbandingan Recuva Data *Recovery* dan Stellar Phoenix Windows Data *Recovery*

No	Parameter	Recuva	Stellar
1	Jumlah data yang berhasil di *Scan*	10	10
2	Jumlah data yang berhasil di *recovery*	10	10

Berdasarkan Tabel 2 diketahui bahwa kedua *toolkit* yang digunakan dapat menemukan semua *file* yang sudah dihapus dan dapat memulihkan kembali semua *file* yang sudah dihapus tersebut.

4. KESIMPULAN

Berdasarkan penelitian yang telah dilakukan dapat disimpulkan bahwa :

1. *Toolkit* Recuva Data *Recovery* dan Stellar Phoenix Windows Data *Recovery* dapat menemukan semua *file* yang sudah dihapus dalam sebuah *flash drive* dan sudah dikosong dari *recycle bin*.
2. *Toolkit* Recuva Data *Recovery*dan Stellar Phoenix Windows Data *Recovery* dapat memulihkan semua *file* yang sudah dihapus dalam sebuah *flash drive*.

5. SARAN

Saran untuk pengembangan dalam penelitian selanjutnya yaitu :

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

DAFTAR PUSTAKA

[1] T. EMS, *Mengatasi Data Hilang dan Serangan Virus*. Jakarta: Elex Media Komputindo, 2009.

[2] B. Mathew, *File Data Recovery : PC Hard drive Data Recovery, USB Data Recovery, Mac Data Recovery, Android Data Recovery, Data Recovery Services*. South Carolina: Createspace Independent Pub, 2014.

[3] I. Lazaridis, T. Arampatzis, and S. Pouros, "Evaluation of Digital Forensics Tools on Data Recovery and Analysis," in *Prosiding The Third International Conference on Computer Science, Computer Engineering and Social Media (CSCESM2016)*, 2016, pp. 67–71.

[4] D. R. Kamblea, N. Jainb, and S. Deshpandec, "Comparison of Digital Forensic Tools Used in DFAI System," *History*, Vol. 2, No. 6, 2015.

[5] F. Sulianta, *Komputer Forensik*. Jakarta: Elex Media Komputindo, 2000.

[6] V. Singh, L. Kesharwani, V. Saran, A. K. Gupta, E. P. Lal, and A. Verma, "Efficacy of Open Source Tools for Recovery of Unconventionally Deleted Data for Forensic Consideration," *Int. J. Sos. Relev. Concern (IJSRC)*, Vol. 3, No. 9, pp. 53–59, 2015.