

PERBANDINGAN KINERJA *ERASER TOOLS* DALAM PENGHAPUSAN DATA YANG AMAN

Yogi Pratama¹, Chairul Mukmin²

Fakultas Ilmu Komputer, Universitas Bina Darma

Email: yogiikk26@gmail.com¹, shairulmukmin@binadarma.ac.id²

ABSTRACT

Computers are a technology device that plays a very important role in productivity in both work and entertainment environments. Over time and the development of information technology, especially in the work environment, requires companies to have computers to support each user in doing their work. The use of computers in the world of work has many positive things, such as facilitating data processing and media with certain applications and the internet to find information. The most common data loss is logical failure, which is when the operating system fails to recognize the file system, whether a disk, a partition or because of a damaged operating system. There are ways to recover lost data by means of data recovery. Data recovery is restoring the lost files and then moving them to a safe place by copying or copying them. Then the process after data recovery can be followed up by repartitioning the hard disk and moving valuable data to another place continuously. Mainly separated from where the operating system is located. At the same time many users are not aware that deleting files or data does not mean destroying the information they contain. To maintain the security of this data, one way is to delete important data from the storage media. However, a truly safe deletion method is needed in carrying out the deletion, so that the data that has been deleted cannot be recovered. From this, we need a method that can make deletion of the data completely safe and not easy to recover with eraser tools.

Keywords: *Eraser Tools, Recovery Data*

ABSTRAK

Komputer merupakan salah satu perangkat teknologi yang berperan sangat penting dalam produktivitas baik dalam lingkungan kerja maupun hiburan, seiring berjalannya waktu dan semakin berkembangnya teknologi informasi terutama dalam lingkungan kerja membuat perusahaan harus memiliki komputer untuk mendukung setiap pengguna dalam melakukan pekerjaannya. Penggunaan komputer dalam dunia kerja memiliki banyak hal yang positif seperti memudahkan pengolahan data dan media dengan aplikasi tertentu serta adanya internet untuk mencari informasi. Kehilangan data yang paling banyak terjadi umumnya adalah kegagalan logis, yaitu ketika sistem operasi gagal untuk mengenali sistem file, baik disk, partisi atau karena sistem operasinya yang rusak. Ada cara untuk mengembalikan data yang hilang dengan cara recovery data. Recovery data adalah mengembalikan file yang sudah hilang tersebut kemudian memindahkannya ke tempat yang aman dengan cara menyalin atau mengcopy. Kemudian proses setelah recovery data bisa ditindak lanjuti dengan pemartisian ulang hard disk dan memindahkan data-data yang berharga ke tempat lain secara terus menerus. Terutama dipisahkan dari tempat sistem operasi berada. Pada saat yang sama pengguna banyak tidak sadar bahwa menghapus file atau data tidak berarti melenyapkan informasi yang dikandungnya. Untuk menjaga keamanan data tersebut, salah satu caranya yaitu dengan melakukan penghapusan data penting tersebut dari media penyimpanan. Namun diperlukan cara penghapusan yang benar-benar aman dalam melakukan penghapusan tersebut, agar data yang telah dihapus tidak

dapat dipulihkan kembali. Dari hal tersebut, diperlukan sebuah metode yang dapat membuat penghapusan data tersebut benar-benar aman dan tidak mudah untuk dipulihkan dengan eraser tools.

Kata Kunci: *Eraser Tools, Recovery Data.*

1. PENDAHULUAN

Komputer merupakan salah satu perangkat teknologi yang berperan sangat penting dalam produktivitas baik dalam lingkungan kerja maupun hiburan, seiring berjalannya waktu dan semakin berkembangnya teknologi informasi terutama dalam lingkungan kerja membuat perusahaan harus memiliki komputer untuk mendukung setiap pengguna dalam melakukan pekerjaannya. Penggunaan komputer dalam dunia kerja memiliki banyak hal yang positif seperti memudahkan pengolahan data dan media dengan aplikasi tertentu serta adanya internet untuk mencari informasi. Selain efek positif tersebut penggunaan komputer juga memiliki efek negatifnya. Sistem operasi komputer menghasilkan berlebihan jumlah data tentang aktivitas penggunanya tersendiri seperti menyimpan informasi penting yang dimiliki, tentunya akan memunculkan resiko yang menjadikan data atau informasi yang ada dalam komputer akan dimiliki oleh orang yang tidak berhak atas data tersebut.

Kehilangan data yang paling banyak terjadi umumnya adalah kegagalan logis, yaitu ketika sistem operasi gagal untuk mengenali sistem file, baik disk, partisi atau karena sistem operasinya yang rusak. Ada cara untuk mengembalikan data yang hilang dengan cara recovery data. Recovery data adalah mengembalikan file yang sudah hilang tersebut kemudian memindahkannya ke tempat yang aman dengan cara menyalin atau mengcopy. Kemudian proses setelah recovery data bisa ditindak lanjuti dengan pemartisian ulang hard disk dan memindahkan data- data yang berharga ke tempat lain secara terus menerus. Terutama dipisahkan dari tempat sistem operasi berada. Pada saat yang sama pengguna banyak tidak sadar bahwa menghapus file atau data tidak berarti melenyapkan informasi yang dikandungnya. Untuk menjaga keamanan data tersebut, salah satu caranya yaitu dengan melakukan penghapusan data penting tersebut dari media penyimpanan. Namun diperlukan cara penghapusan yang benar-benar aman dalam melakukan penghapusan tersebut, agar data yang telah dihapus tidak dapat dipulihkan kembali. Dari hal tersebut, diperlukan sebuah metode yang dapat membuat penghapusan data tersebut benar-benar aman dan tidak mudah untuk dipulihkan dengan eraser tools. Dalam penelitian ini akan diuji kinerja beberapa eraser tools yang telah dipilih sebelumnya untuk dianalisa kelebihan dan kekurangannya, baru kemudian dibandingkan hasil keamanan data antara eraser tools tersebut.

2. METODOLOGI PENELITIAN

2.1 Komputer Forensik

Saat ini teknologi komputer dapat digunakan sebagai alat bagi para pelaku kejahatan komputer: seperti pencurian, penggelapan uang dan lain sebagainya. Barang bukti yang berasal dari komputer telah muncul dalam persidangan hampir 30 tahun. Awalnya, hakim menerima bukti tersebut tanpa membedakannya dengan bentuk bukti lainnya. Namun seiring dengan kemajuan teknologi komputer, perlakuan tersebut menjadi membingungkan. Bukti yang berasal dari komputer sulit dibedakan antara yang asli ataupun salinannya, karena berdasarkan sifat alaminya, data yang ada dalam komputer sangat mudah dimodifikasi. Proses pembuktian bukti tindak kejahatan tentunya memiliki kriteria-kriteria, demikian juga dengan proses pembuktian pada bukti yang didapat dari komputer. Di awal tahun 1970-an Kongres Amerika Serikat mulai merealisasikan kelemahan hukum yang ada dan mencari solusi terbaru yang lebih cepat dalam penyelesaian kejahatan komputer. US Federal Rules of Evidence 1976 menyatakan permasalahan

tersebut [1].

2.2 Anti Forensik

Anti Forensik merupakan istilah yang digunakan bagi pelaku kejahatan untuk membuat sulit para investigator dalam melakukan investigasi barang bukti digital baik di TKP ataupun di Laboratorium Forensics. Menurut Rogers (2006), Anti Forensik merupakan usaha untuk menimbulkan efek negatif terhadap keberadaan dan kualitas dari barang bukti dari lokasi kejadian, atau membuat sebuah proses analisa barang bukti menjadi susah dilakukan [2].

2.3 Eraser Tools

Eraser tools adalah proses penghapusan data permanen, dimana file atau data yang telah dihapus tidak akan bisa kembali. Beda halnya dengan recovery data yang mengembalikan file atau data dari kondisi yang rusak gagal, korup atau tidak bisa diakses ke kondisi awal yang normal.

2.4 Recovery Data

Menurut Tim EMS, *Recovery* data 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 mengembalikan data yang hilang maka proses data recovery ini bisa digunakan dalam konteks komputer forensik atau untuk mata- mata [3].

3. HASIL DAN PEMBAHASAN

Pada bab ini berisi tentang pembahasan dan hasil penelitian dan melakukan pengujian dari tiap-tiap aplikasi *eraser tools* agar mendapatkan perbandingan. Hal ini bertujuan agar mengetahui aplikasi mana yang terbaik dalam penghapusan data yang aman.

3.1 Hasil Penelitian

Untuk mendapatkan hasil yang diinginkan dan melihat data yang telah dilakukan penghapusan menggunakan aplikasi *eraser tools*, maka pengujian ini membutuhkan bantuan dari aplikasi *recovery* data yang ada untuk melihat proses pengembalian data yang dilihat pada saat penghapusan, dan dapat menentukan aplikasi mana yang dapat memenuhi dari kebutuhan tersebut. Berikut tools yang digunakan untuk recovery data.

3.2 Hasil Pengujian Kinerja Eraser Tools

Pengujian ini dilakukan untuk mengetahui bagaimana kinerja tools dalam penghapusan data di dalam sebuah *hard disk*. Dalam pengujian ini akan dilihat kinerja dan kecepatan *eraser tools*, dan akan dilakukan pengembalian data yang telah dilakukan penghapusan menggunakan aplikasi *recovery* data. Hasilnya berdasarkan banyaknya jumlah data yang dapat dipulihkan menggunakan *recovery* data. Dalam melakukan kinerja *eraser tools* dibutuhkan suatu lingkungan pengujian yang dibangun untuk mendapatkan data. Berdasarkan kebutuhan forensik yang harus dipenuhi *eraser tools*, maka di dalam *hard disk* terdapat file-file yang akan digunakan untuk melakukan penghapusan menggunakan aplikasi *eraser tools*, berikut.

Tabel 1. Spesifikasi Data

No	Nama File	Tipe File	Ukuran File
1	A	Docx	5.41 MB

2	B	Pdf	1.56 GB
3	C	Pptx	6.23 KB
4	D	Mkv	1.56 GB
5	E	Avi	7.72 MB
6	F	Mp4	60.1 MB
7	G	Jpg	80.2 KB
8	H	Gif	199 KB
9	I	Png	11.1 KB

Hasil pengujian kecepatan penghapusan aplikasi *eraser tools* menggunakan Metode "Waktu Jam" henti /stopwatch maka diperoleh hasil seperti tabel berikut.

Tabel 2. Hasil Pengujian Kecepatan Penghapusan Eraser Tools

Aplikasi	Type File	Ukuran File	Time Left	Keterangan
<i>Wipe File</i> 2.3	Docx	5.41 MB	2 menit 20 detik	Waktu didapat setelah melakukan penghapusan file dan pengujian penghitungan kecepatan sebanyak 3 kali dari 9 file yang dihapus maka didapatkan hasil waktu 2 menit 20 detik
	Pdf	1.56 GB		
	Ppt	6.23 KB		
	Mkv	1.56 GB		
	Avi	7.72 MB		
	Mp4	60.1 MB		
	Jpeg	80.2 KB		
	Gif	199 KB		
	Png	11.1 KB		
<i>File Shredder</i> 2.50	Docx	5.41 MB	3 menit 11 detik	Waktu didapat setelah melakukan penghapusan file dan pengujian penghitungan kecepatan sebanyak 3 kali dari 9 file yang dihapus maka didapatkan hasil waktu 3 menit 11 detik
	Pdf	1.56 GB		
	Ppt	6.23 KB		
	Mkv	1.56 GB		
	Avi	7.72 MB		
	Mp4	60.1 MB		
	Jpeg	80.2 KB		
	Gif	199 KB		
	Png	11.1 KB		
<i>Dp Wiper</i> 1.1	Docx	5.41 MB	3 menit 35 detik	Waktu didapat setelah melakukan penghapusan file dan pengujian penghitungan kecepatan sebanyak 3 kali dari 9 file yang dihapus maka didapatkan hasil waktu 3 menit 35 detik
	Pdf	1.56 GB		
	Ppt	6.23 KB		
	Mkv	1.56 GB		
	Avi	7.72 MB		
	Mp4	60.1 MB		
	Jpeg	80.2 KB		
	Gif	199 KB		
	Png	11.1 KB		

<i>Cyber Shredder 1.12</i>	Docx	5.41 MB	3 menit 14 detik	Waktu didapat setelah melakukan penghapusan file dan pengujian penghitungan kecepatan sebanyak 3 kali dari 9 file yang dihapus maka didapatkan hasil waktu 2 menit 20 detik
	Pdf	1.56 GB		
	Ppt	6.23 KB		
	Mkv	1.56 GB		
	Avi	7.72 MB		
	Mp4	60.1 MB		
	Jpeg	80.2 KB		
	Gif	199 KB		
	Png	11.1 KB		
<i>Eraser 5.7</i>	Docx	5.41 MB	7 menit 11 detik	Waktu didapat setelah melakukan penghapusan file dan pengujian penghitungan kecepatan sebanyak 3 kali dari 9 file yang dihapus maka didapatkan hasil waktu 3 menit 11 detik
	Pdf	1.56 GB		
	Ppt	6.23 KB		
	Mkv	1.56 GB		
	Avi	7.72 MB		
	Mp4	60.1 MB		
	Jpeg	80.2 KB		
	Gif	199 KB		
	Png	11.1 KB		

3.3 Hasil Perbandingan Tools Yang Digunakan Untuk Recovery

Untuk mendapatkan hasil yang diinginkan, maka dibutuhkan suatu perbandingan aplikasi eraser tools yang ada untuk melihat proses penghapusan data yang dilihat pada saat penghapusan, kemudian melakukan pemulihan data menggunakan aplikasi recovery data agar dapat menentukan aplikasi mana yang dapat memenuhi dari kebutuhan tersebut.

1) **Recuva 1.5.3**

- 1) Setelah melakukan pengujian untuk mengembalikan data, hasil pengembalian data menggunakan *Recuva 1.5.3* untuk mengembalikan data yang telah dilakukan penghapusan data menggunakan *Wipe File 2.3* tidak ada data yang bisa dikembalikan.
- 2) Setelah melakukan pengujian untuk mengembalikan data, hasil pengembalian data menggunakan *Recuva 1.5.3* untuk mengembalikan data yang telah dilakukan penghapusan data menggunakan *FileShredder 2.50* tidak ada data yang bisa dikembalikan.
- 3) Setelah melakukan pengujian untuk mengembalikan data, hasil pengembalian data menggunakan *Recuva 1.5.3* untuk mengembalikan data yang telah dilakukan penghapusan data menggunakan *Dp Wiper 1.1* tidak ada data yang bisa dikembalikan
- 4) Setelah melakukan pengujian untuk mengembalikan data, hasil pengembalian data menggunakan *Recuva 1.5.3* untuk mengembalikan data yang telah dilakukan penghapusan data menggunakan *Cyber Shredder* tidak ada data yang bisa dikembalikan
- 5) Setelah melakukan pengujian untuk mengembalikan data, hasil pengembalian data menggunakan *Recuva 1.5.3* untuk mengembalikan data yang telah dilakukan penghapusan data menggunakan *Eraser 5.7* tidak ada data yang bisa dikembalikan.

2) **Puran File Recovery 1.21**

- 1) Setelah melakukan pengujian untuk mengembalikan data, hasil pengembalian data menggunakan *Puran File Recovery 1.21* untuk mengembalikan data yang telah dilakukan penghapusan data menggunakan *Wipe File 2.3* tidak ada data yang bisa dikembalikan.
- 2) Setelah melakukan pengujian untuk mengembalikan data, hasil pengembalian data menggunakan *Puran File Recovery 1.21* untuk mengembalikan data yang telah dilakukan penghapusan data menggunakan *File Shredder 2.50* tidak ada data yang bisa dikembalikan.
- 3) Setelah melakukan pengujian untuk mengembalikan data, hasil pengembalian data

menggunakan Puran File Recovery 1.21 untuk mengembalikan data yang telah dilakukan penghapusan data menggunakan Dp Wiper 1.1 tidak ada data yang bisa dikembalikan

- 4) Setelah melakukan pengujian untuk mengembalikan data, hasil pengembalian data menggunakan Puran File Recovery 1.21 untuk mengembalikan data yang telah dilakukan penghapusan data menggunakan Cyber Shredder 1.12 tidak ada data yang bisa dikembalikan
- 5) Setelah melakukan pengujian untuk mengembalikan data, hasil pengembalian data menggunakan Puran File Recovery 1.21 untuk mengembalikan data yang telah dilakukan penghapusan data menggunakan *Eraser* 5.7 tidak ada data yang bisa dikembalikan.

3) **Mini Tool Partition Recovery 8.7**

- 1) Setelah melakukan pengujian untuk mengembalikan data, hasil pengembalian data menggunakan Mini Tool Partition Recovery 8.7 untuk mengembalikan data yang telah dilakukan penghapusan data menggunakan Wipe File 2.3 tidak ada data yang bisa dikembalikan.
- 2) Setelah melakukan pengujian untuk mengembalikan data, hasil pengembalian data menggunakan Mini Tool Partition Recovery 8.7 untuk mengembalikan data yang telah dilakukan penghapusan data menggunakan File Shredder 2.50 tidak ada data yang bisa dikembalikan.
- 3) Setelah melakukan pengujian untuk mengembalikan data, hasil pengembalian data menggunakan Mini Tool Partition Recovery 8.7 untuk mengembalikan data yang telah dilakukan penghapusan data menggunakan Dp Wiper 1.1 tidak ada data yang bisa dikembalikan
- 4) Setelah melakukan pengujian untuk mengembalikan data, hasil pengembalian data menggunakan Mini Tool Partition Recovery 8.7 untuk mengembalikan data yang telah dilakukan penghapusan data menggunakan Cyber Shredder 1.12 tidak ada data yang bisa dikembalikan.
- 5) Setelah melakukan pengujian untuk mengembalikan data, hasil pengembalian data menggunakan Mini Tool Partition Recovery 8.7 untuk mengembalikan data yang telah dilakukan penghapusan data menggunakan *Eraser* 5.7 tidak ada data yang bisa dikembalikan.

4) **Restoration 2.5.14**

- 1) Setelah melakukan pengujian untuk mengembalikan data, hasil pengembalian data menggunakan Restoration 2.5.14 untuk mengembalikan data yang telah dilakukan penghapusan data menggunakan Wipe File 2.3 tidak ada data yang bisa dikembalikan.
- 2) Setelah melakukan pengujian untuk mengembalikan data, hasil pengembalian data menggunakan Restoration 2.5.14 untuk mengembalikan data yang telah dilakukan penghapusan data menggunakan File Shredder 2.50 tidak ada data yang bisa dikembalikan.
- 3) Setelah melakukan pengujian untuk mengembalikan data, hasil pengembalian data menggunakan Restoration 2.5.14 untuk mengembalikan data yang telah dilakukan penghapusan data menggunakan Dp Wiper 1.1 tidak ada data yang bisa dikembalikan
- 4) Setelah melakukan pengujian untuk mengembalikan data, hasil pengembalian data menggunakan Restoration 2.5.14 untuk mengembalikan data yang telah dilakukan penghapusan data menggunakan Cyber Shredder 1.12 tidak ada data yang bisa dikembalikan
- 5) Setelah melakukan pengujian untuk mengembalikan data, hasil pengembalian data menggunakan Restoration 2.5.14 untuk mengembalikan data yang telah dilakukan penghapusan data menggunakan *Eraser* 5.7 tidak ada data yang bisa dikembalikan.

5) **Pandora Recovery 2.0.289**

- 1) Setelah melakukan pengujian untuk mengembalikan data, hasil pengembalian data menggunakan Pandora Recovery 2.0.289 untuk mengembalikan data yang telah dilakukan

- penghapusan data menggunakan Wipe File 2.3 tidak ada data yang bisa dikembalikan.
- 2) Setelah melakukan pengujian untuk mengembalikan data, hasil pengembalian data menggunakan Pandora Recovery 2.0.289 untuk mengembalikan data yang telah dilakukan penghapusan data menggunakan File Shredder 2.50 tidak ada data yang bisa dikembalikan.
 - 3) Setelah melakukan pengujian untuk mengembalikan data, hasil pengembalian data menggunakan Pandora Recovery 2.0.289 untuk mengembalikan data yang telah dilakukan penghapusan data menggunakan Dp Wiper 1.1 tidak ada data yang bisa dikembalikan
 - 4) Setelah melakukan pengujian untuk mengembalikan data, hasil pengembalian data menggunakan Pandora Recovery 2.0.289 untuk mengembalikan data yang telah dilakukan penghapusan data menggunakan Cyber Shredder 1.12 tidak ada data yang bisa dikembalikan
 - 5) Setelah melakukan pengujian untuk mengembalikan data, hasil pengembalian data menggunakan Pandora Recovery 2.0.289 untuk mengembalikan data yang telah dilakukan penghapusan data menggunakan *Eraser 5.7* tidak ada data yang bisa dikembalikan.

3.4 Pembahasan

Berdasarkan hasil pengujian tools yang telah dilakukan maka dapat ditarik kesimpulan bahwa Tools Eraser Tools dapat menghapus data dengan aman, dari pengujian penghapusan dan pengembalian data yang dihapus tidak ada data yang bisa di kembalikan, untuk kecepatan penghapusan yang telah diuji dengan metode "Waktu Jam" henti / stopwatch tools *Wipe File 2.3* adalah tools yang mempunyai kecepatan menghapus lebih unggul dari tools *File Shredder 2.50*, *Dp Wiper 1.1*, *Cyber Shredder 1.12*, dan *Eraser 5.7*.

4. KESIMPULAN

4.1 Kesimpulan

Berdasarkan data yang telah dikumpulkan serta pengujian yang telah dilakukan, maka peneliti dapat mengambil kesimpulan sebagai berikut:

- 1) Kelima aplikasi *eraser tools* yaitu *Wipe File 2.3*, *File Shredder 2.50*, *Dp Wiper 1.1*, *Cyber Shredder 1.12*, *Eraser 5.7* sangat aman untuk melakukan penghapusan, karena setelah mengumpulkan data, melakukan pengujian. Kelima aplikasi ini tidak dapat mengembalikan file- file tertentu seperti dokumen ,gambar, video dan audio. yang dihapus benar-benar tidak dapat kembali.
- 2) Diantara kelima aplikasi setelah dilakukan pengujian kecepatan tools *Wipe File 2.3* mempunyai kecepatan penghapusan data dengan waktu 2 menit 20 detik lebih cepat dibandingkan ke empat aplikasi eraser tools lainnya.

DAFTAR PUSTAKA

- [1] Wikipedia bahasa Indonesia, "Forensik", (2010, Juni 24). Tersedia : <http://wikipedia.org/wiki/forensik>.
- [2] "Anti Forensics Digital". rahmatinggiwares.1 januari 1970. 24 februari 2020. <<https://rahmatinggiwares.blogspot.com/2017/07/anti-forensics-digital-dan-contoh-kasus.html>>.
- [3] D. R. Kamblea, N. Jainb, and S. Deshpandec, "Comparison of Digital Forensic Tools Used in DFAISystem," History, Vol. 2, No. 6, 2015.