Versi Online:
https://journal.ubm.ac.id/index.php/alu
DOI: http://dx.doi.org/10.30813/j-alu.v2i2. 3587

Jurnal Algoritma, Logika dan Komputasi
Vol.V (No. 1) : 436 - 444. Th. 2022
p-ISSN: 2620-620X
e-ISSN: 2621-9840

ANALISA TEKNIK ANTI KOMPUTER FORENSIK MENGGUNAKAN METODE OVERWRITING METADATA PADA DIGITAL EVIDENCE

Analysis Of Anti Computer Forensics Technique Using Overwriting Metadata Method On Digital Evidence

Julian Saputra[1)], Jusia Amanda Ginting[2)]
[1)] Program Studi Informatika/Fakultas Teknologi dan Desain, Universitas Bunda Mulia

ABSTRACT

The development of technology during this globalization period is very fast and rapid, especially during the pandemic in this world which makes all activities like education, work etc. carried out online-based. Because, with the increase in the use of online-based media, a problem arises like crimes that use online or digital media as an intermediary known as cybercrime. With this cybercrime, a science that can be used in securing personal data is needed, namely anti-computer forensic science. This research is focused on the analysis and implementation of forensic anti-computer science in securing personal files. In this study, the anti-computer forensic method that will be analyzed and applied is metadata overwriting, data destruction, and data hiding.In this test, the three methods will be broken down again into several sub methods or techniques such as file obscure manipulation, file timestamp manipulation, secure deletion, and data encryption. The results of the application of several categories of techniques will be written and then analyzed.The results of the study showed that the technique tested was very good and safe in securing personal files so that they could not be detected by systems or digital forensic software but there were still weaknesses, namely in the data hiding section if the password or key used was simple, it would be easy to hack.

Keywords: *Anti Computer Forensics, Metadata Ovewriting, Data Destruction, Data Hiding*

ABSTRAK

Perkembangan teknologi pada masa globalisasi ini sangatlah cepat dan pesat terutama pada saat terjadinya masa pandemi di dunia ini yang membuat semua kegiatan berupa pendidikan, pekerjaan dll dilakukan berbasis online. Tentunya dengan adanya peningkatan penggunaan media berbasis online tersebut timbul suatu masalah berupa tindak kejahatan yang menggunakan media online atau digital sebagai perantaranya yang dikenal cybercrime. Dengan adanya cybercrime tersebut maka diperlukan suatu ilmu yang dapat digunakan dalam mengamankan data pribadi yaitu ilmu anti komputer forensik. Penelitian ini difokuskan pada analisa dan implementasi ilmu anti komputer forensik dalam mengamankan *file* pribadi. Pada penelitian ini metode anti komputer forensik yang akan dianalisa dan diterapkan ialah *overwriting metadata, data destruction,* dan *data hiding.* Pada pengujian ini dari ketiga metode tersebut akan dipecah lagi menjadi beberapa sub metode atau teknik seperti manipulasi *obscure file,* manipulasi *timestamp file, secure deletion,* dan enkripsi *data.* Hasil dari penerapan dari beberapa kategori teknik tersebut akan ditulis lalu akan dianalisa.Hasil dari penelitian menunjukkan bahwa teknik yang diuji sudah sangat cukup baik dan aman dalam mengamankan *file* pribadi agar tidak dapat terdeteksi oleh sistem maupun *software* digital forensik tetapi masih terdapat kelemahan yaitu pada bagian *data hiding* apabila kata sandi atau *key* yang digunakan sederhana maka akan gampang diretas.

Kata Kunci: Anti Komputer Forensik, *Overwriting Metadata, Data Destruction, Data Hiding*

Jurnal Algoritma, Logika dan Komputasi
Vol.V (No. 1) : 436 - 444. Th. 2022
p-ISSN: 2620-620X
e-ISSN: 2621-9840

PENDAHULUAN

Kejahatan di dunia maya marak terjadi disebabkan adanya peningkatan aktivitas dari pengguna internet terkhusus pada masa pandemi covid-19 [1]. Terbukti di Indonesia jumlah pengguna internet aktif pada tahun 2022 ini sebesar 204,7 juta orang [2] dan terus mengalami peningkatan. Hal ini tentu saja dapat menimbulkan dampak negatif terutama dibidang *security*. Tingginya *traffic data* juga meningkatkan resiko terhadap pencurian *data* yang dapat melanggar ketentuan peratuan perundang-undangan di Indonesia. Dengan perkembangan teknologi yang sangat pesat ini, manusia tentunya sangat diuntungkan dan juga dirugikan, dengan adanya perkembangan teknologi ini manusia dimudahkan dalam mengakses internet secara bebas dan luas begitupun sebaliknya muncul suatu kekhawatiran dalam penggunaan akses internet yang bebas yaitu dimana manusia dapat membuka, maupun mengunduh *software-software* secara mudah dan gratis. Apabila ditinjau lebih lanjut tentang penggunaan *software*, mau itu *software* komputer forensik ataupun *software* dengan fungsi yang lain, semuanya bersifat netral. Netral Artinya tergantung dari penggunanya, bisa digunakan untuk melakukan hal-hal yang positif dan juga hal-hal negatif. Bila dilihat dari sisi positif penggunaan *software-software* komputer forensik sangatlah membantu sang investigator atau kriptanalisis dalam menganalisis dan mengidentifikasi suatu barang bukti digital, tetapi apabila dilihat dari sisi negatifnya *software* komputer forensik ini dapat disalahgunakan seperti *merecovery* kembali *file-file*, *log* orang lain untuk menyebar aib ataupun menjatuhkan orang lain.

Dari pemaparan latar belakang diatas dapat diketahui bahwa tindak kejahatan cybercrime khususnya pada kasus pencurian *data* yang dilakukan oleh oknum maupun individu sangat merugikan bagi masyarakat. Oleh karena itu diperlukan suatu penelitian berupa uji coba atau implementasi ilmu anti komputer forensik yang bertujuan untuk mengamankan data pribadi yang tidak dapat diakes oleh siapapun selain pemiliknya itu sendiri, maka dari itu dapat dirumuskan masalahnya yaitu bagaimana mengimplementasi serta menganalisa ilmu anti komputer forensik menggunakan beberapa teknik atau metode anti komputer forensik seperti *overwriting metadata, data desctruction, dan data hiding.*

Penulis berharap dengan adanya implementasi serta analisa metode anti komputer forensik ini dapat membantu masyarakat dalam memilih teknik anti komputer forensik yang baik dan aman untuk mengamankan *data-data* pribadi.

METODE PENELITIAN

Metode *Overwriting Metadata*

Overwriting metadata merupakan salah satu teknik atau metode dari bidang anti komputer forensik. Alur atau cara kerja dari metode *overwriting metadata* ini ialah dengan cara mengubah maupun memodifikasi atau memanipulasi *timestamp file* dan *log file* pada *data*. Memanipulasi suatu file merupakan suatu rangkaian atau proses rekayasa dengan cara kerja melakukan penambahan, penggantian, penyembunyian, serta penghapusan terhadap bagian dari suatu file. *Overwriting Metadata* juga biasa dikenal dengan sebutan memanipulasi file. [3] [4].

Metode *Data Desctruction*

Dikutip dari TechTarget bahwa *data destruction* atau merusak *data* merupakan suatu proses penghancuran *data* yang disimpan pada *disk, harddisk*, dan bentuk media elektronik yang lainnya sehingga membuat *data* yang berada dalam media elektronik tersebut tidak dapat diakses maupun dibaca [5]. Pada metode *data destruction* ini, tekniknya dibagi menjadi beberapa sub teknik atau metode lagi seperti:

secure deletion atau disebut juga *Wiping* merupakan suatu proses menghapus *data* dengan aman sehingga *data* yang

Jurnal Algoritma, Logika dan Komputasi
Vol.V (No. 1) : 436 - 444. Th. 2022
p-ISSN: 2620-620X
e-ISSN: 2621-9840

dihapus tersebut tidak dapat dikembalikan atau dipulihkan kembali dengan *software recovery data* [6].

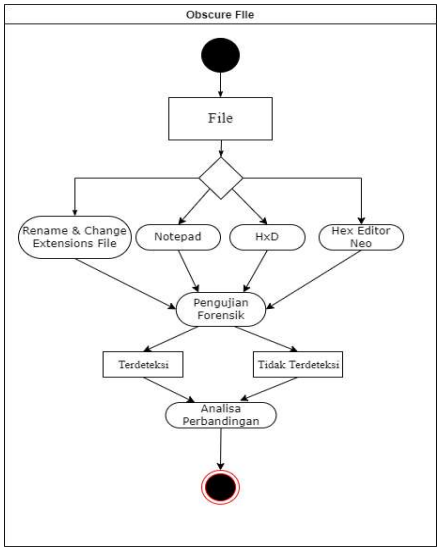
Changing MAC Attributes merupakan proses mengubah dan menghapus elemen atau atribut waktu pada *file* yang membuat *file* tersebut tidak dapat dianalisa waktunya.

Metode *Data Hiding*

Data Hiding merupakan teknik untuk menyembunyikan suatu *data* menggunakan metode meng-enkripsi *data*, menyisipkan *data* atau *file* tersebut kedalam *file* lain [7]. Dalam metode *data hiding* ini, tekniknya dibagi menjadi beberapa sub teknik atau metode lagi seperti:

Kriptografi merupakan suatu metode yang digunakan untuk menyembunyikan isi sebuah pesan dengan cara *data* atau pesan tersebut diberikan sandi atau enkripsi sedemikian rupa sehingga isi pesan tersebut tidak dapat diketahui isinya.

Steganografi merupakan suatu metode atau ilmu menyembunyikan sebuah pesan atau informasi dengan cara menyisipkan suatu pesan kedalam pesan lain atau suatu objek/media yang dapat berupa gambar, teks, video, musik, maupun media digital yang lainnya [8].



Gambar 1. *Activity Diagram Obscure File*

Compression Bombs merupakan suatu metode yang digunakan untuk memperlambat laju investigasi. Cara kerja dari metode *compression bombs* ini sangat mirip dengan *DDoS Attack* yaitu menghabiskan sumber daya suatu sistem [9]. Proses nya ialah membuat serta menyisipkan *file* yang ukurannya besar lalu dikompresi seolah-olah terlihat seperti *file* dengan ukuran yang kecil, Tetapi pada saat dibuka atau dilakukan *uncompress, file* tersebut akan mengkonsumsi sumber daya sistem tersebut sehingga membuat *tools* maupun sistem yang digunakan menjadi *crash* atau rusak.

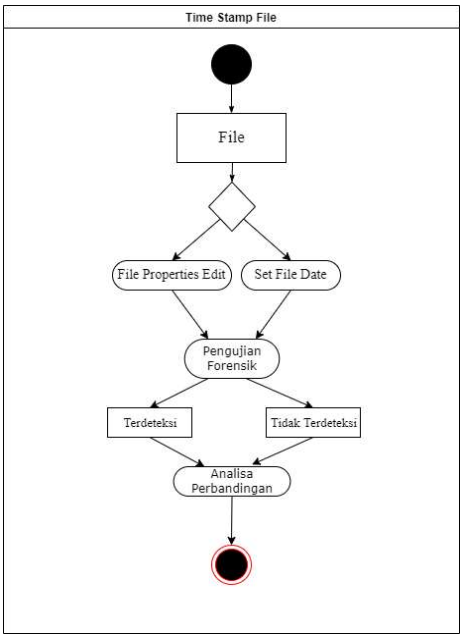
HASIL & PEMBAHASAN

Pemilihan Metode

Dalam melakukan uji coba implementasi dan analisa ilmu anti komputer forensik pada *digital evidence*. Berikut merupakan sub teknik atau metode dari *overwriting metadata, data destruction,* dan *data hiding* yang akan digunakan, sebagai berikut:

1. *Overwriting Metadata*
   - Obscure file seperti yang ditunjuk pada Gambar 1 merupakan suatu teknik penyamaran file dengan cara merubah nama file, ekstensi file, ataupun merubah ASCII header yang terdapat dalam sebuah file menggunakan software atau tools-tools anti komputer forensik. Dalam percobaan ini akan dilakukan simulasi proses menyamarkan file dengan teknik merubah nama serta ekstensi dari file dan akan dilakukan pengujian forensik menggunakan software atau tools komputer forensik, apakah nanti hasilnya file tersebut masih terdeteksi atau tidak. Jika file tersebut masih terdeteksi maka akan dilakukan teknik atau metode obscure file yang lain sampai file tersebut benar-benar tidak terdeteksi atau berhasil mengelabui software komputer forensik dan apabila file atau digital evidence tersebut masih terdeteksi maka akan dibuat suatu kesimpulan. Berikut

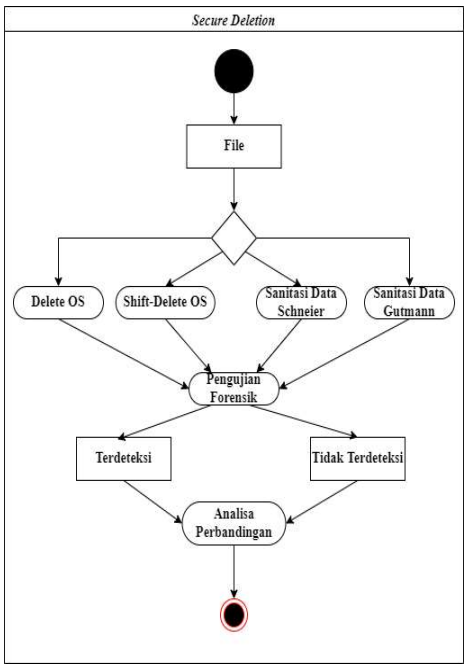
merupakan alur atau struktur kerja dari teknik obscure file seperti yang ditunjukkan pada Gambar 1



Gambar 2 *Activity Diagram Timestamp File*

- Manipulasi *timestamp file*

Merupakan suatu teknik penyamaran dengan cara menyamarkan waktu file yang ada pada bagian properties file seperti created, modified, dan accessed. Pada percobaan implementasi teknik ini akan menggunakan software anti komputer forensik sebagai bantuan untuk merubah pencacatan waktunya dan selanjutnya melakukan pengujian dengan software komputer forensik apakah sudah tidak terdeteksi atau masih terdeteksi perubahan yang telah dilakukan. Jika terdeteksi maka akan melakukan percobaan yang selanjutnya sampai file yang diuji tersebut berhasil tidak terdeteksi, dan apabila file atau digital evidence tersebut masih terdeteksi maka akan dibuat suatu kesimpulan. Apabila file yang diuji sudah tidak terdeksi maka akan uji coba lebih lanjut menggunakan teknik lain guna mengukur, membedakan atau menganalisis tingkat perbandingan satu teknik dengan teknik yang lainnya. Berikut merupakan alur atau struktur kerja dari teknik penyamaran *timestamp file* seperti yang ditunjukkan pada Gambar 2



Gambar 3 *Activity Diagram Secure Deletion*

2. *Data Destruction*

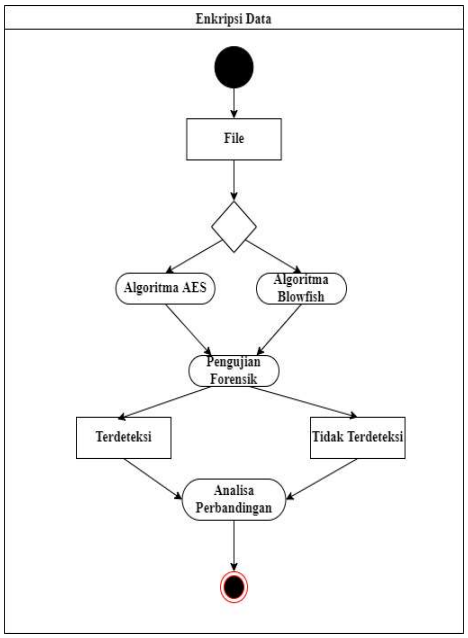
Secure Deletion merupakan suatu teknik anti komputer forensik yang bertujuan untuk menyembunyikan *data* dengan aman. Proses atau alur kerja dari *secure deletion* ini ialah dengan cara menghapus file secara aman sehingga *file* tersebut tidak dapat dikembalikan atau *direcovery* kembali oleh *software-software recovery.* Pada percobaan teknik *secure deletion* ini akan dilakukan percobaan dengan menggunakan cara menghapus biasa, *shift-delete*, maupun menggunakan beberapa bantuan *software* anti komputer forensik, Apabila hasil dari percobaan pada *file* tersebut masih dapat terdeteksi oleh sistem komputer maka akan dilakukan uji coba lain sampai *file* tidak dapat

Jurnal Algoritma, Logika dan Komputasi
Vol.V (No. 1) : 436 - 444. Th. 2022
p-ISSN: 2620-620X
e-ISSN: 2621-9840

terdeteksi oleh sistem komputer, dan apabila *file* atau *digital evidence* tersebut masih terdeteksi maka akan dibuat suatu kesimpulan. Tahap selanjutnya, apabila *file* sudah tidak dapat terdeteksi maka akan dilakukan percobaan lain untuk mendapatkan analisis perbandingan dari teknik ataupun *software* anti komputer forensik yang digunakan. Berikut merupakan alur atau struktur dari teknik *secure deletion,* seperti yang ditunjukkan pada gambar 3.

3. *Data Hiding*

Enkripsi *data* merupakan suatu salah satu teknik dari bagian metode *data hiding* yang tujuannya untuk mengamankan *data* dengan cara menyembunyikan *data* tersebut. Proses atau alur kerja dari *encrypted data* ini ialah dengan cara mengkonversi *data* menjadi kode-kode rahasia sehingga *data* tersebut menjadi aman dan terlindungi. Pada percobaan teknik *encrypted data* ini akan dilakukan percobaan dengan bantuan beberapa bantuan *software*. Apabila hasil dari percobaan pada *file* tersebut masih dapat terdeteksi oleh sistem komputer maka akan dilakukan uji coba lagi menggunakan software yang lain sampai *file* tidak dapat terdeteksi oleh sistem komputer. dan apabila *file* atau *digital evidence* tersebut masih terdeteksi maka akan dibuat suatu kesimpulan. Tahap selanjutnya, walaupun *file* sudah tidak dapat terdeteksi oleh sistem pada komputer maka akan dilakukan percobaan lagi menggunakan *software* lain untuk mendapatkan analisis perbandingan dari *software* yang digunakan. Berikut merupakan alur atau struktur dari teknik enkripsi *data,* seperti yang ditunjukkan pada Gambar 4



Gambar 4 *Activity Diagram* Enkripsi *Data*

Hasil Pengujian Metode

Hasil uji coba pengujian dan kesimpulan dari beberapa metode yang telah dipilih dan diuji coba. Hasil uji coba pengujian akan disajikan kedalam bentuk tabel seperti Tabel 1

Tabel 1 Hasil Uji Coba *Obscure File*

Tahap	Teknik yang digunakan	*Software*	Hasil	Pengujian Forensik
Tahap 1	Manipulasi nama & ekstensi file	-	Gagal	-
Tahap 2	Manipulasi *signature file*	Notepad	Berhasil	Gagal
Tahap 3	Manipulasi *signature file*	HxD	Berhasil	Berhasil (Tidak Terdeteksi)
Tahap 4	Manipulasi *signature file*	Hex Editor Neo	Berhasil	Berhasil (Tidak Terdeteksi)

Berdasarkan dari uji coba *obscure file* serta pengujian forensiknya dapat disimpulkan

Jurnal Algoritma, Logika dan Komputasi
Vol.V (No. 1) : 436 - 444. Th. 2022
p-ISSN: 2620-620X
e-ISSN: 2621-9840

bahwa teknik *obscure file* dengan melakukan mengubah atau manipulasi nama serta ekstensi *file* serta mengubah *signature file* atau ASCII *header file* dapat membuat file tersebut tidak dapat terdeteksi oleh *tools* atau *software* digital forensik yang membuat teknik *obscure file* ini cukup baik dalam mengamankan suatu *file* pribadi yang sifatnya penting atau rahasia. Diperagakanpada Tabel 2

Tabel 2 Hasil Uji Coba Manipulasi *Timestamp File*

Tahap	Pengujian Forensik	*Software* yang digunakan
Tahap 1	Berhasil (Tidak Terdeteksi)	*File Properties Edit*
Tahap 2	Berhasil (Tidak Terdeteksi)	*Set File Date*

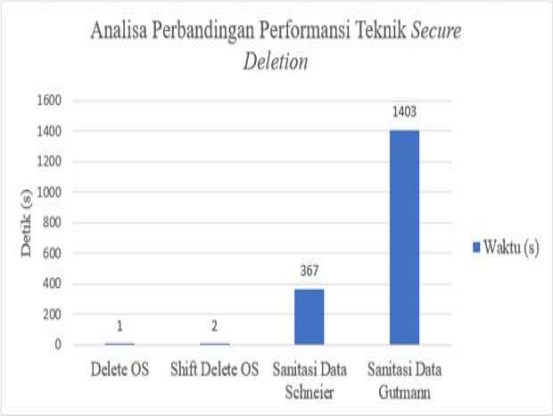
Dari kedua tahapan uji coba penelitian manipulasi *timestamp* atau pencatatan waktu pada *file* tidak dapat menampilkan contoh nyata terjadinya kegagalan (berhasil terdeteksi oleh software forensik) dikarenakan terbatasnya ruang lingkup berupa penggunaan software digital forensik dalam melakukan pengujian forensik. Dengan hasil uji seperti pada Tabel 3.

Tabel 3 Hasil Uji Coba *Secure Deletion*

Tahap	Teknik yang digunakan	*Software* yang digunakan	Pengujian Forensik
Tahap 1	*Delete* OS	-	Gagal (Terdeteksi oleh sistem/*software)*
Tahap 2	*Shift-delete* OS	-	Gagal (Terdeteksi oleh sistem/*software)*
Tahap 3	Metode sanitasi *data schneier*	*Eraser*	Berhasil (Tidak terdeteksi)
Tahap 4	Metode sanitasi *data gutmann*	*Eraser*	Berhasil (Tidak terdeteksi)

Data Desctruction:

Analisa perbandingan dari keempat teknik *secure deletion* yang telah diuji. *Data* yang diuji untuk melakukan uji coba *secure deletion* ini ialah sebesar 10,3 GB dengan *file atau digital evidence* sebanyak 3065 *file* dengan berbagai macam kategori atau ekstensi. Berikut merupakan perbandingan dari masing-masing teknik *secure deletion* yang diukur dari segi performansi waktu. Seperti pada grafik yang ditunjukkan pada Gambar 5.



Gambar 5. Grafik Perbandingan Performansi Waktu Teknik *Secure Deletion*

Dari gambar 5 memperlihatkan bahwa metode *delete* OS dan metode *shift-delete* OS mempunyai waktu yang sangat singkat dalam melakukan penghapusan yaitu sebesar 1 dan 2 detik dibandingkan dengan metode sanitasi *data* schneier dan gutmann, sedangkan dari kedua metode sanitasi *data* tersebut, *schneier* masih lebih unggul dari segi perfomansi waktu dibandingkan dengan *gutmann.*

Tahap analisa selanjutnya ialah melakukan uji perbandingan *recovery data* dengan cara membandingkan jumlah *file* atau *digital evidence* yang dapat dipulihkan beserta total ukurannya. Berikut merupakan jumlah *file* atau *digital evidence* yang telah berhasil dipulihkan kembali, seperti yang ditunjukkan pada Tabel 4.

Jurnal Algoritma, Logika dan Komputasi
Vol.V (No. 1) : 436 - 444. Th. 2022
p-ISSN: 2620-620X
e-ISSN: 2621-9840

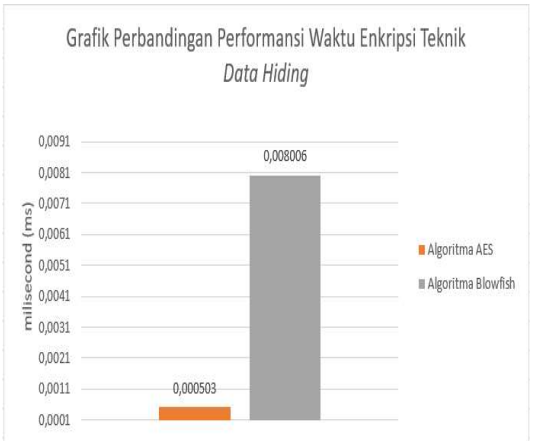
Tabel 4 Hasil Perbandingan jumlah *file* yang berhasil *direcoveru*

No	Metode yang digunakan	*Software Recovery yang digunakan*	Jumlah *file yang berhasil direcovery*	
			Loadable	Size
1	*Delete* OS	*Recycle bin*	3065	10,3 GB
2	*Shift-delete* OS	*Recuva*	3063	10,3 GB
3	Metode sanitasi *data schneier*	*Recuva*	0	6,78 MB
4	Metode sanitasi *data gutmann*	*Recuva*	0	2,73 MB

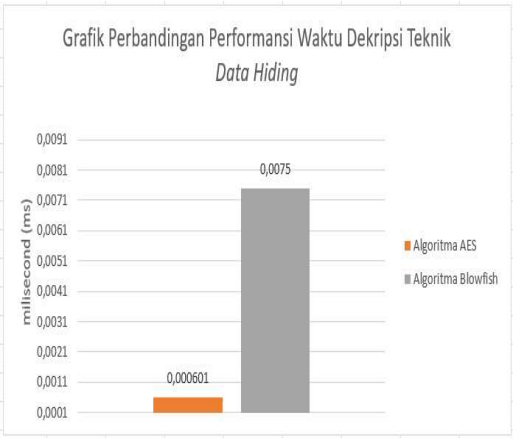
Pada tabel 4 dapat dijelaskan bahwa semua *file* yang diuji menggunakan teknik *secure deletion* dengan *Delete* OS dan *Shift-delete* OS dapat dibuka dan dibaca secara normal setelah *direcovery*, sedangkan pada *file* yang diuji menggunakan teknik *secure deletion* dengan metode sanitasi *data schneier* dan *Gutmann* tidak terdapat satupun file yang dapat dibuka dan dibaca kembali. Apabila dilihat dari ukuran *file* yang berhasil *direcovery*, ini dikarenakan *file* yang dapat *direcovery* ialah *file metadata* dari *NTFS* dan *junk file* yang tidak mempunyai tipe atau ekstensi. Kesimpulan dari hasil diatas adalah uji coba *secure deletion* menggunakan teknik sanitasi *data schneier* dan *Gutmann* cukup aman untuk menghilangkan *file* atau *digital evidence* pada media penyimpanan.

Data Hiding:

Pada uji coba ini algoritma serta jenis algoritma yang akan diuji coba ialah algoritma kunci simetris menggunakan 2 jenis algoritma yaitu Algoritma *AES* dan Algoritma *Blowfish*, pada uji coba ini *digital evidence* yang akan digunakan berupa *file* dengan isi berupa *teks*. Proses pengujian akan dilakukan sebanyak 20 perulangan, Menurut Jacob Nielsen pengujian sebanyak 20 kali perulangan mempunyai tingkat kepercayaan sebanyak 90% [10], karena itu dalam melakukan uji coba ini akan dilakukan sebanyak 20 kali perulangan untuk mengurangi tingkat kesalahan atau *margin of error*. Berikut merupakan perbandingan dari masing-masing teknik enkripsi *data* yang diukur dari segi performansi waktu. Seperti pada grafik yang ditunjukkan pada Gambar 6 dan Gambar 7.



Gambar 6. Perbandingan Waktu Enkripsi



Gambar 7. Perbandingan Waktu Dekripsi

Berdasarkan dari gambar 6 dan 7 diatas dapat disimpulkan bahwa apabila ditinjau dari perfomansi waktu atau tingkat kecepatan proses enkripsi dan dekripsi antara algoritma *AES* dan *Blowfish* dapat disimpulkan bahwa algoritma *AES* mempunyai proses enkripsi dan dekripsi yang tercepat atau terbilang singkat

dibandingkan dengan algoritma *Blowfish*.

SIMPULAN

Berdasarkan penelitian yang sudah dilakukan penulis menyimpulkan bahwa:

1. Teknik *obscure file*, dengan melakukan manipulasi *file* berupa mengubah nama serta ekstensi *file,* dan mengubah *signature file* pada *file* atau *digital evidence* membuat *file* atau *digital evidence* tersebut menjadi tidak dapat terdeteksi oleh *software* atau *tools* digital forensik yang membuat teknik *obscure file* ini cukup baik dalam mengamankan suatu *file* pribadi yang sifatnya penting atau rahasia.
2. Teknik *timestamp file,* dengan melakukan manipulasi *file* tepatnya pada bagian *timestamp* atau pencatatan waktu *file* menggunakan bantuan *software* atau tools
   Timestamp Editor tentunya sangat membantu dalam mengamankan *file* pribadi karena dengan adanya manipulasi *timestamp* ini dapat merusak integritas atau keaslian suatu *file* dan juga dengan terbatasnya ruang lingkup berupa kurangnya atau minimnya *software* digital forensik dalam mendeteksi suatu perubahan *metadata* berupa *timestamp file* membuat teknik ini cukup baik dalam mengamankan *file* pribadi.
3. *Data Destruction,* kesimpulan dalam melakukan uji coba *data destruction secure deletion* ialah dengan melakukan *secure deletion* menggunakan teknik sanitasi *data schneier* dan *gutmann*, kedua teknik tersebut sangat cukup baik dan aman dalam melakukan penghapusan *file-file* pribadi yang sifatnya penting dikarenakan dengan menggunakan kedua teknik sanitasi data ini, *file* diuji tersebut tidak dapat *direcovery* kembali menggunakan bantuan *software* digital forensik.
4. Teknik *Data Hiding,* dengan melakukan teknik *data hiding* berupa enkripsi *data* ini tentunya sangat membantu dalam mengamankan *file* pribadi yang sifatnya rahasia tetapi dalam melakukan enkripsi data ini mempunyai satu kelemahan yaitu apabila kata sandi atau key yang digunakan untuk mengenkripsi suatu *file* tersebut sangat sederhana, tentunya sangat mudah dipecahkan atau diretas menggunakan metode *bruteforce*. Maka dari itu dalam melakukan enkripsi atau pengamanan data menggunakan kata sandi atau key direkomendasikan menggunakan kata sandi atau key yang rumit atau sulit.

DAFTAR PUSTAKA

[1] Y. Prianto, N. A. Fuzain, and A. Farhan, "Kendala Penegakan Hukum Terhadap Cyber Crime Pada Masa Pandemi Covid-19," *Prosiding SENAPENMAS*, no. 21, p. 1111, 2021, doi: 10.24912/psenapenmas.v0i0.15146.

[2] P. D. Liberty Jemadu, "Jumlah Pengguna Internet Indonesia Capai 204,7 Juta di Tahun 2022," *www.suara.com*, 2022. https://www.suara.com/tekno/2022/02/21/163932/jumlah-pengguna-internet-indonesia-capai-2047-juta-di-tahun-2022?page=all (accessed Apr. 19, 2022).

[3] A. Jain and G. S. Chhabra, "Anti-Forensics Techniques : An Analytical Review," 2014.

[4] S. Garfinkel, "Anti-forensics: Techniques, detection and countermeasures," *ICIW 2007: 2nd International Conference on i-Warfare and Security*, no. January 2007, pp. 77–84, 2007.

[5] "What Is Data Destruction," *www.blancco.com*, 2019. https://www.blancco.com/resources/article-data-destruction-definition/#:~:text=TechTarget defines data destruction as "the

process of,with most data protection standards%2C you need more. (accessed Mar. 13, 2022).

[6] "What Is Digital Forensics?," *https://ilmuforensicsku.wordpress.com/*. https://ilmuforensicsku.wordpress.com/2017/08/02/anti-forensik/ (accessed Mar. 13, 2022).

[7] M. J. Joel, "THE ANTI-FORENSICS TACTICS, TECHNIQUES, AND PROCEDURES (TTPs) CYBERCRIMINALS USE TO HIDE ELECTRONIC EVIDENCE OF CRIMES," *THE ANTI-FORENSICS TACTICS, TECHNIQUES, AND PROCEDURES (TTPs) CYBERCRIMINALS USE TO HIDE ELECTRONIC EVIDENCE OF CRIMES*, no. May, 2019.

[8] S. R. Widianto, "Desain Algoritma Steganografi dengan Metode Spread Spectrum Berbasis PCMK (Permutasi Chaotic Multiputaran Mengecil dan Membesar) Yang Tahan Terhadap Gangguan," *Prosiding Seminar Nasional Sains dan Teknologi*, pp. 1–8, 2018.

[9] D. A. Arifah, "KASUS CYBERCRIME DI INDONESIA Indonesia's Cybercrime Case," *Jurnal Bisnis dan Ekonomi (JBE)*, vol. 18, no. 2, pp. 185–195, 2011.

[10] Nielsen Norman Group, "Quantitative Studies: How Many Users to Test," 2006, [Online]. Available: https://www.nngroup.com/articles/quantitative-studies-how-many-users/