JIKO (Jurnal Informatika dan Komputer)
Vol. 7, no. 2, September 2023, hal. 296–300
e-ISSN : 2477-3964 — p-ISSN : 2477-4413
DOI: dx.doi.org/10.26798/jiko.v7i2.692

PENYEMBUNYIAN DATA MENGGUNAKAN METODE OVERWRITING METADATA

Julian Saputra[1] dan **Jusia Amanda Ginting**[2]
[1,2]Program Studi Informatika/Fakultas Teknologi dan Desain, Universitas Bunda Mulia, Indonesia
Email: julian089697@gmail.com[1], jginting@bundamulia.ac.id[2]

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 uji coba ilmu metode overwriting metadata dan hasilnya akan dianalisa tingkat efektifitasannya dari uji coba penelitian menggunakan metode overwriting metatada tersebut dalam mengamankan file pribadi. Hasil dari penerapan dari beberapa metode tersebut akan ditulis lalu akan dianalisa tingkat ke-efektifitasannya. Hasil dari penelitian menunjukkan bahwa penelitian menggunakan metode overwriting metadata mempunyai tingkat ke-efektifitas yang cukup baik dan aman dalam mengamankan file pribadi. Hal ini ditunjukkan dari file yang diuji tidak dapat terdeteksi oleh software atau tools digital forensik dan juga dengan terbatasnya ruang lingkup berupa kurangnya atau minimnya software digital forensik dalam mendeteksi suatu perubahan metadata membuat metode ini cukup baik dalam mengamankan data atau file pribadi.
Kata Kunci: *Anti Komputer Forensik, Overwriting Metadata*

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 scientific trials of the metadata overwriting method and the results will be analyzed for its effectiveness from the research trials using the metadata overwriting method in securing personal files. The results of the application of some of these methods will be written and their effectiveness will be analyzed. The results of the study indicate that research using the metadata overwriting method has a fairy good and safe level of effectiveness in securing personal files. This is shown from the files being tested cannot be detected by software or digital forensic tools and also with the limited scope in the form of the lack or lack of digital forensic software in detecting a metadata change, making this method quite good in securing personal data or files.
KeyWords: *Anti Komputer Forensik, Overwriting Metadata*

I. 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. Dilansir dari media detik *finance* direktur keamanan siber dan sandi keuangan perdagangan dan pariwisata (BSSN) pihaknya telah merangkum beberapa fenomena kasus pencurian data yang terjadi pada tahun 2021-2022 ini, salah satunya ialah kasus pencurian data yang dialami oleh *BRI Life* yang tejadi pada bulan juli 2021 yang lalu dimana hampir 2 juta data dicuri dan dijual melalui media atau *forum online* [3]. Dengan adanya fenomena ini tentunya masyarakat sangat khawatir dan dirugikan dengan adanya kasus pencurian data ini, tentunya masalah ini dapat diminimalisir atau dicegah dengan cara yang sederhana terlebih dahulu salah satunya ialah mengamankan data personal sendiri di media lokal pada perangkat masing-masing. 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. Dengan adanya fenomena ini pasti kesadaran

JIKO (Jurnal Informatika dan Komputer)
Vol. 7, no. 2, September 2023, hal. 296–300
e-ISSN : 2477-3964 — p-ISSN : 2477-4413
DOI: dx.doi.org/10.26798/jiko.v7i2.692

masyarakat pengguna internet akan bangun untuk meminimalisir kejadian ini dimulai dari hal-hal yang kecil salah satunya ialah mengamankan data personal dimedia lokal pada perangkat masing-masing. Pertanyaannya ialah bagaimana melakukannya? Oleh karena itu diperlukan suatu penelitian berupa uji coba penyembunyian data menggunakan metode anti komputer forensik, salah satu teknik penerapannya ialah menggunakan metode *overwriting* metadata dan akan dilakukan analisa bagaimana ke-efektifitasan dari penerapan metode *overwriting* metadata yang di-uji tersebut, maka dari itu dapat dirumuskan masalahnya yaitu bagaimana mengimplementasi serta menganalisa ke-efektifitasan menggunakan metode *overwriting* metadata. Dengan adanya implementasi serta analisa bagaimana ke-efektifitasan metode yang diuji ini, dapat membantu masyarakat dalam memilih teknik anti komputer forensik yang baik dan aman untuk mengamankan data-data pribadi.

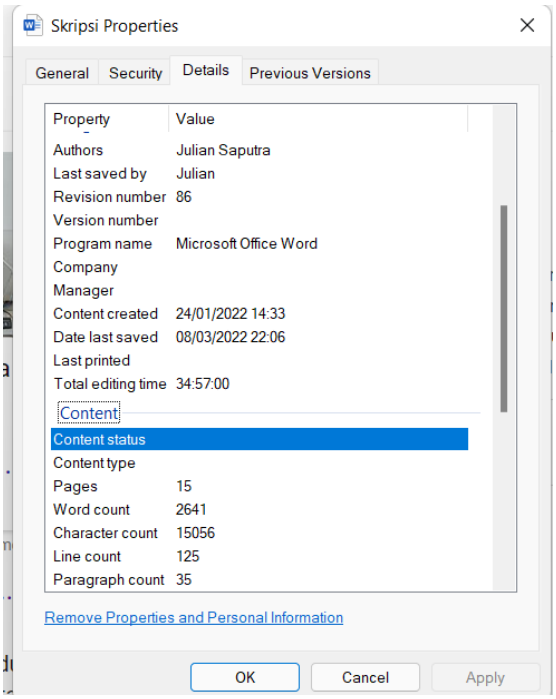
II. Landasan Teori

A. *Anti Komputer Forensik*

Anti Komputer Forensik merupakan kebalikan dari Komputer Forensik yang dimana komputer forensik lebih mengarah untuk mencari, mengidentifikasi, serta menjaga suatu integritas atau keaslian suatu bukti/data, tetapi pada Anti Komputer Forensik lebih berfokus pada cara menjaga agar suatu data tersebut menjadi aman serta tidak dapat diakses oleh orang lain selain pemilik dari data tersebut [4]. Anti Komputer Forensik juga merupakan suatu metode yang digunakan untuk mempersulit maupun menggagalkan sang investigator forensik dalam melaksanakan atau memecahkan kasus yang berhubungan dengan digital forensik [5], [6].

B. *Metadata*

Metadata merupakan suatu informasi yang terstruktur untuk mendeskripsikan, menemukan atau menjadikan suatu informasi menjadi mudah untuk dikelola. sedangkan menurut ALA (*American Library Association*) [7]. *Metadata* merupakan suatu data yang terstruktur serta ditandai dengan kode agar dapat diproses dengan mudah di komputer, serta membantu identifikasi, penilaian, pengelolaan satuan pembawa informasi. Fungsi atau tujuan adanya metadata yang terdapat pada suatu file ialah metadata dapat digunakan untuk mengidentifikasi sumber yang mempunyai elemen atau karakter yang unik yang membuat file tersebut berbeda dari satu sumber dengan yang lainnya. Serta metadata digunakan juga untuk mengelola sumber [8]. Informasi pada file tentunya bersifat *fragile* yang berarti barang tersebut dapat mengalami kerusakan atau formatnya dapat berubah yang membuat informasi digital menjadi tidak relevan dan tidak dapat digunakan lagi dalam proses pengadilan [9]. Fungsi *metadata* sebagai pengelola sumber sangat berperan penting pada bagian ini dikarenakan sifat dari *metadata* itu sendiri yaitu menggunakan sistem pengarsipan dan preservasi untuk membantu menyimpan, menjaga supaya sumber informasi dari suatu file tersebut tetap aman [8], [10]. Contoh yang sangat mudah mengenai *metadata* ialah pada dokumen atau file yang terdapat pada *Microsoft Word*, seperti pada Gambar 1 berikut:



Gambar 1: Elemen-elemen pada *metadata*

JIKO (Jurnal Informatika dan Komputer)
Vol. 7, no. 2, September 2023, hal. 296–300
e-ISSN : 2477-3964 — p-ISSN : 2477-4413
DOI: dx.doi.org/10.26798/jiko.v7i2.692

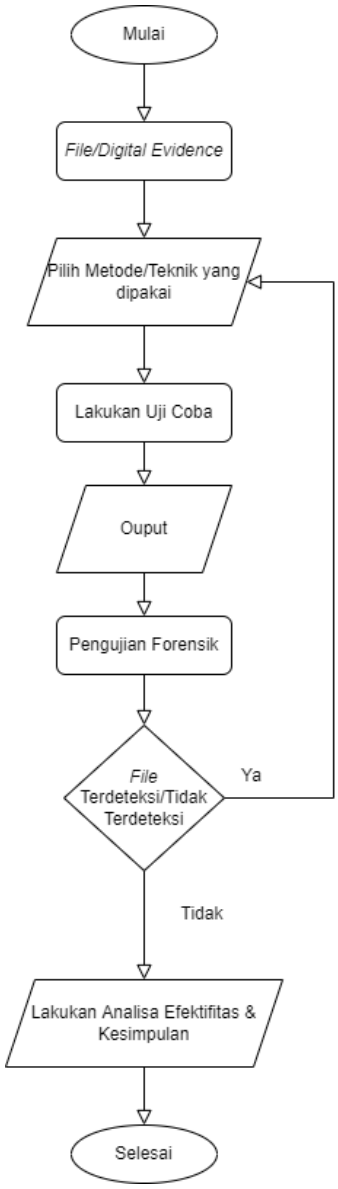
Pada Gambar 1 berupa dokumen *Microsoft word* diatas mempunyai beberapa informasi apa saja yang termasuk ke dalam elemen-elemen penyusun informasi atau data yang terletak pada bagian *properties* lalu pada tab detail di dokumen *Microsoft word* mengenai metadata yaitu siapa penulisnya, data terakhir disimpan oleh siapa, nama program, kapan konten dibuat, serta total waktu mengedit.

C. 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 [11], [12].

III. Analisa dan Perancangan

Dibawah ini merupakan gambaran alur atau jalan kerja dari uji coba penyembunyian data yang akan disajikan dalan tampilan flowchart seperti pada Gambar 2:



Gambar 2: *Flowchart* Alur Uji Coba Penyembunyian Data

Berikut merupakan teknik atau metode dari overwriting metadata yang akan digunakan, sebagai berikut:

JIKO (Jurnal Informatika dan Komputer)
Vol. 7, no. 2, September 2023, hal. 296–300
e-ISSN : 2477-3964 — p-ISSN : 2477-4413
DOI: dx.doi.org/10.26798/jiko.v7i2.692

a. Obscure file 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.
b. 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.

Dalam melakukan uji coba penelitian penyembunyian data menggunakan metode *overwriting* metadata ini dibutuhkan bantuan berupa *software-software* forensik yang tersedia oleh sistem ataupun oleh pihak ketiga, pada uji coba *overwriting* metadata ini digunakan bantuan *software* forensik seperti pada Tabel I berikut:

Tabel I: Analisa Kebutuhan Software

		Software	
No	**Tools/Software**	**Tools/Software Version**	**Link Download**
1	File Investigator Tools	V 3.37	https://file-investigator-file-find-for-windows.updatestar.com/
2	Hex Editor Neo	V 6.54.02.6790	https://www.hhdsoftware.com/free-hex-editor
3	Set File Date	V 2.0	https://setfiledate.en.softonic.com/download
4	File Properties Edit	V 3.75	https://download.cnet.com/File-Property-Edit-Free/3000-2248_4-75345208.html

IV. Hasil dan Pembahasan

Berikut merupakan hasil uji coba pengujian dari uji coba penyembunyian data menggunakan metode *overwriting* metadata. Hasil uji coba pengujian akan disajikan kedalam bentuk Tabel II seperti berikut:

Tabel II: 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 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.

Tabel III: 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.

V. Simpulan

Berdasarkan penelitian yang sudah dilakukan penulis menyimpulkan bahwa tingkat ke-efektifitasan dari uji coba menggunakan metode *overwriting* metadata ini sangat baik dan aman untuk mengamankan suatu file. Hal ini ditunjukkan dari file yang diuji tidak dapat terdeteksi oleh *software* atau *tools digital* forensik dan juga dengan terbatasnya ruang lingkup berupa kurangnya atau minimnya *software digital* forensik dalam mendeteksi suatu perubahan *metadata* membuat metode ini cukup baik dalam mengamankan data atau file pribadi.

JIKO (Jurnal Informatika dan Komputer)
Vol. 7, no. 2, September 2023, hal. 296–300
e-ISSN : 2477-3964 — p-ISSN : 2477-4413
DOI: dx.doi.org/10.26798/jiko.v7i2.692

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] S. Fatimah, "sederet-kasus-kebocoran-data-yang-landa-ri-selama-pandemi-covid-19." [Online]. Available: https://finance.detik.com/moneter/d-5795754/sederet-kasus-kebocoran-data-yang-landa-ri-selama-pandemi-covid-19
[4] Arrywan, Eko, and C. SmithDev, Anti Forensik: Mengatasi Investigasi Komputer Forensik. Elex Media Komputindo, 2010. [Online]. Available: http://www.bukabuku.com/browses/product/9789792788884/anti-forensik-mengatasi-investigasi-komputer-forensik.html?msclkid=a167872bc02d11ecbf33eca6fcdec569
[5] W. Li, "Anti-forensic Digital Investigation for Unauthorized Intrusion on a Wireless Network," 2013.
[6] W. Erfan, "Definisi Dan Teknik Anti Komputer Forensik Manajemen Investigasi Tindak Kriminal," pp. 2–4, 2016.
[7] "Metadata," American Library Association, 2010. http://www.ala.org/tools/atoz/metadata/metadata (accessed Mar. 10, 2022).
[8] "Metadata adalah? Fungsi dan Jenis-Jenis Metadata," appkey.id, 2020. https://appkey.id/pembuatan-website/backend/metadata-adalah/ (accessed Mar. 10, 2022).
[9] I. O, D. Chris, and D. David, "A New Approach of Digital Forensic Model for Digital Forensic Investigation," International Journal of Advanced Computer Science and Applications, vol. 2, no. 12, pp. 175–178, 2011, doi: 10.14569/ijacsa.2011.021226.
[10] Wikipedia.org, "Metadata." https://id.wikipedia.org/wiki/Metadata?msclkid=ddb1546ac03511ecad892aa60aabba58 (accessed Mar. 11, 2022).
[11] A. Jain and G. S. Chhabra, "Anti-Forensics Techniques: An Analytical Review," 2014.
[12] 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.