OPEN ACCESS
J. OF ICT, VOL. 3, NO. 1, PP.020-030, JUNE 2021

ISSN : 2686-1089 (ONLINE)

Journal of Informatics and Communications Technology (JICT)

Analisis Keamanan Perangkat Lunak Enkripsi Media Penyimpanan DiskCryptor

Rana Zaini Fathiyana [1], Sutoro[2], Yan Hadynoer [3], Dinda Jaelani Hidayat[4]

1) *Akademi Teknik Telekomunikasi Sandhy Putra Jakarta*
Jl. Daan Mogot KM.11 Kedaung Kali Angke, Cengkareng, Jakarta Barat, Indonesia
[1] ranazainifathiyana@gmail.com

[2,3)] *Badan Siber dan Sandi Negara, Jakarta*
[2] torotoxx@gmail.com, [3] hadynoer@gmail.com
Jl. Harsono RM No.70, Ragunan, Kec. Ps. Minggu, Jakarta Selatan, Indonesia

[4)]*Badan Meteorologi Klimatologi dan Geofisika, Jakarta*
[4] jaelanidinda@gmail.com
Jl. Angkasa 1 No.2, Gn. Sahari, Kec. Kemayoran, Jakarta Pusat, Indonesia

Abstract

Penggunaan komputer atau laptop memberikan manfaat dalam meningkatkan produktivitas dan efisiensi kerja, namun menghadirkan implikasi lain yang belum menjadi atensi yaitu resiko kehilangan data. *Full disk encryption* merupakan salah satu solusi ideal untuk menjaga kerahasiaan dan keamanan data yang tersimpan pada *hard disk* komputer atau laptop. Pada sistem operasi Windows terdapat aplikasi enkripsi yang popular digunakan, yaitu DiskCryptor. Namun, sampai sejauh mana layanan keamanan yang diberikan aplikasi DiskCryptor dan adakah kelemahan dari desain dan implementasi yang memungkinkan timbulnya celah keamanan terhadap data yang dilindungi. Pada penelitian ini membahas analisis keamanan aplikasi DiskCryptor dilihat dari sudut pandang penggunaan algoritma enkripsi ataupun dekripsi, penggunaan kunci, analisis waktu, serta data forensik.

Keywords: Enkripsi, *Full Disk Encryption*, *DiskCryptor*, Forensik.

I. INTRODUCTION

Facebook kembali tertimpa masalah pencurian data. Sebanyak 29.000 data informasi finansial karyawan Facebook, yang mencakup data lengkap karyawan, data gaji, informasi bank dan informasi lainnya yang tersimpan di dalam sejumlah *hard disk* yang tidak terenkripsi telah dicuri [1]. Selain itu, pada tanggal 8 Mei 2017, *Covered Entity* (CE), *Bay Area Pain and Wellness Center*, menemukan bahwa mesin *Electromyography* (EMG) yang tersimpan di mobil karyawan telah dicuri. Sebuah laptop yang terpasang pada EMG berisi informasi kesehatan elektronik atau *electronic protected health information* (ePHI) dari sekitar 548 pasien. ePHI berisi data nama pasien dan tanggal lahir. Laptop tersebut telah dilindungi *password* namun tidak dienkripsi [2]. Meningkatnya popularitas penggunaan laptop dalam lingkungan perusahaan memberikan

dampak positif bagi peningkatan produktivitas dan efisiensi, namun menimbulkan dampak lainnya yaitu terjadinya resiko kehilangan data yang signifikan. Perangkat ini dapat dengan mudah hilang atau dicuri. Walaupun harga laptop tersebut tidak seberapa dibandingkan dengan nilai data yang tersimpan di dalamnya.

Teknologi enkripsi merupakan jawaban kebutuhan keamanan data perusahaan, melindungi data seperti di laptop atau komputer *desktop*, media penyimpanan *removable*, dan lain-lain. Enkripsi secara signifikan dapat mengurangi atau menghilangkan risiko bisnis yang terkait dengan pelanggaran yang mengakibatkan pengungkapan data rahasia. Enkripsi terbagi menjadi beberapa metode yaitu: *file encryption, volume encryption* dan *full disk encryption*.

Full disk encryption (FDE) merupakan solusi untuk menjaga kerahasiaan data yang tersimpan pada perangkat portabel atau laptop. Dengan FDE memungkinkan seluruh kapasitas dan data pada *hard drive* komputer akan diubah menjadi bentuk yang hanya bisa dimengerti oleh orang yang memiliki kunci untuk mendeskripsi data yang telah dienkripsi. Setelah *hard drive* terenkripsi, pengguna perlu *login* ketika komputer pertama kali dinyalakan ini disebut dengan proses *Pre-Boot Authentication*, dapat dengan cara memasukan *password*, atau menggunakan token (*smartcard* atau USB). Telah banyak dikembangkan perangkat lunak FDE seperti TrueCrypt, VeraCrypt, BitLocker, dan DiskCryptor.

Pada penelitian ini akan dibahas mengenai salah satu perangkat lunak FDE yaitu DiskCryptor. DiskCryptor adalah perangkat lunak enkripsi pada *hard drive* yang mempunyai Lisensi Publik Umum GNU untuk sistem operasi Windows. Bahasan difokuskan terhadap analisis keamanan aplikasi DiskCryptor yang dilihat dari sudut pandang penggunaan algoritma enkripsi ataupun dekripsi, penggunaan panjang kunci, analisis waktu, serta data forensik.

II. LITERATURE REVIEW

Olson, 2021 pada [3] telah melakukan sebuah penelitian untuk mengukur *(benchmark)* performa baca dan tulis dari tiga aplikasi enkripsi yang semuanya menggunakan algoritma enkripsi simetris AES, Twofish, dan Serpant. Ketiga aplikasi enkripsi tersebut adalah TrueCrypt, BestCrypt dan DiskCryptor. *Benchmark* dimaksudkan untuk membandingkan hasil pengukuran performa pada tiga aplikasi enkripsi tersebut. *Benchmark* dilakukan menggunakan aplikasi tambahan yaitu Anvil's Storage Utilities 1.0.34 Beta 11, yang mana dapat digunakan untuk mengukur performa baca dan tulis pada *hard disk* mekanis dan perangkat *solid state* (SSD). Pengujian dilakukan pada sistem operasi Windows 7 64 bit dengan kondisi semua aplikasi yang tidak berkaitan dengan pengukuran *benchmark* di non-aktifkan terlebih dahulu agar tidak mempengaruhi hasil pengukuran *benchmark*. Pada pengujian *benchmark* dari ketiga aplikasi ini diterapkan pada tiga *hard disk* mekanis dan satu perangkat *solid state* (SSD). Penelitian tersebut menjadi dasar bagi penulis untuk melakukan penelitian lebih khusus untuk aplikasi enkripsi *hard disk* DiskCryptor. Penelitian yang dilakukan akan menguji penggunaan mode operasi, penggunaan panjang kunci, analisis waktu enkripsi dan dekripsi, serta melakukan uji forensik.

A. *Aplikasi Enkripsi Hard Disk*

Salah satu bentuk pengamanan yang dapat diterapkan untuk sebuah media penyimpanan adalah dengan menggunakan aplikasi enkripsi. Aplikasi enkripsi untuk media penyimpanan menggunakan algoritma simetrik dengan menggunakan kunci yang sama untuk proses enkripsi maupun dekripsi. Proses enkripsi dapat dilakukan dengan 3 (tiga) metode berbeda, yaitu *software-based*, *controller-based*, dan *internal disk encryption*. Salah satu yang umum digunakan adalah dengan metode *software-based encryption* untuk enkripsi media penyimpanan. Dengan metode *software-based encryption*, proses enkripsi dapat diterapkan untuk *file* atau *folder*, *volume*, atau bahkan keseluruhan media [3].

a) *File encryption* diterapkan berdasarkan pada bagaimana proses enkripsi/dekripsi hanya untuk sebuah atau beberapa *file* atau *folder* di dalam media penyimpanan (*disk*) dengan menerapkan otentikasi untuk akses terhadap *file* yang telah dienkripsi.

b) *Volume encryption* merupakan sebuah proses enkripsi yang dilakukan terhadap *volume* yang ada di dalam media penyimpanan (C:\, D:\, E:\, dan seterusnya). Konsep dari *volume encrption* ini adalah dimana *file* atau *folder* di dalam *volume* hanya dapat diakses atau dibaca apabila *volume* yang dipakai sudah didekripsi.

c) *Full disk encryption* adalah proses enkripsi yang diterapkan pada sebuah media penyimpanan fisik utuh baik itu yang sudah terpasang di dalam PC atau *notebook* ataupun yang bersifat portabel (USB, *hard disk* eksternal). Enkripsi dijalankan untuk keseluruhan data yang ada di dalam media penyimpanan baik itu *file*, *folder*, program, aplikasi atau bahkan sistem operasi. Metode *full disk encryption* umumnya menggunakan sebuah *user interface* berupa *boot loader* untuk akses terhadap media penyimpanan (dekripsi) dengan mekanisme otentikasi.

B. DiskCryptor

DiskCryptor adalah sebuah program *open source* yang menawarkan enkripsi semua partisi *disk* (termasuk partisi sistem) untuk Microsoft Windows. Pada awalnya DiskCryptor dirancang untuk menggantikan sistem enkripsi *disk* komersial seperti DriveCrypt Plus Pack dan PGP Whole Disk Encryption, dan menggunakan algoritma AES-256, Twofish, Serpent atau kombinasi algoritma bertingkat dalam mode XTS untuk melakukan enkripsi.

Sejak awal tahun 1990, *full disk encryption* komersial telah hadir untuk Microsoft DOS. TrueCrypt muncul di tahun 2004 sebagai perangkat lunak *open source* utama, dalam perkembangannya pada tahun 2008 TrueCrypt menghendaki enkripsi dari *system drive* yang diimplementasikan di versi 5. Namun beberapa bulan sebelum peluncuran TrueCrypt, pengguna TrueCrypt dan anggota forum yang menggunakan nama 'ntldr' (anonim) mengembangkan suatu program *open source* yang mampu mengenkripsi *system drive* pada Microsoft Windows: DiskCryptor.

Menurut pengembang pada awalnya DiskCryptor (rilis 0.1-0.4) sepenuhnya kompatibel dengan format *container* TrueCrypt karena menggunakan format partisi dan data terenkripsi yang sesuai dengan algoritma AES-256 dalam mode LRW. Namun, dimulai dari DiskCryptor 0.5 terjadi peningkat pada format yang memungkinkan enkripsi data pada Windows XP, untuk memungkinkan sistem partisi memiliki format yang sama persis dengan non-sistem partisi dan untuk mendukung rencana proyek di masa depan [4].

C. Algoritma Kriptografi

Menurut Schneier, 1996 kriptografi adalah ilmu sekaligus seni untuk menjaga keamanan pesan. Kriptografi bertujuan untuk mengamankan informasi yang akan disimpan atau ditansmisikan dalam bentuk tertentu dengan proses enkripsi. Enkripsi adalah proses menyandikan *plain text* (format teks yang dapat dibaca) menjadi *cipher text* (format teks yang tidak dapat dibaca oleh *eavesdropper* atau penyadap). Sedangkan proses dimana mengubah karakter informasi dari teks yang tidak dapat dibaca *(cipher text)* menjadi teks yang dapat dibaca *(plain text).*

DiskCryptor mendukung algoritma enkripsi AES-256, Twofish dan Serpent. Selain itu pengguna juga dapat memilih untuk menggunakan kombinasi algoritma bertingkat yang akan menjaga data tetap aman meskipun ada salah satu algoritma yang akan dipatahkan. Sistem enkripsi penyimpanan menggunakan kunci simetris, yaitu menggunakan kunci yang sama untuk enkripsi dan dekripsi. Perbedaan dari macam-macam algoritma enkripsi seperti pada Tabel I di bawah ini:

TABLE I
PERBEDAAN ALGORITMA ENKRIPSI

Algoritma	Desainer Algoritma	Ukuran Kunci (Bit)	Ukuran Blok (Bit)
AES	J. Daemen, V. RIjmen	256	128
Serpent	R. Anderson, E. Biham, L. Knudsen	256	128
Twofish	B. Schneier, J. Kelsey, D. Whiting, D. Wagner, C. Hall, N. Ferguson	256	128
AES-Twofish		256, 256	128
Twofish-Serpent		256,256	128
Serpent-AES		256, 256	128
AES-Twofish-Serpent		256, 256, 256	128

Algoritma yang digunakan DiskCryptor mendukung bit kunci dan blok yang sama, yakni ukuran kunci 256 bit dan *block cipher* simetris 128 bit. DiskCryptor juga mendukung penggunaan enkripsi bertingkat dengan menggunakan ketiga algoritma kriptografi AES, Twofish dan Serpent.

a. AES-Twofish, setiap blok 128 bit pertama dienkripsi dengan Twofish (256 bit) dan kemudian dengan AES (256 bit) keduanya dalam mode operasi XTS. XTS menggunakan dua kunci independen untuk kepentingan yang berbeda.
b. Twofish-Serpant, Setiap 128 bit blok pertama dienkripsi dengan Serpent (256 bit) pada mode operasi XTS setelah itu dienkripsi lagi dengan Twofish (256 bit) pada mode operasi XTS.
c. Serpent-AES, Dua *cipher* beroperasi dalam mode XTS, dengan setiap *cipher* memiliki kunci independen. Setiap blok 128 bit pertama dienkripsi dengan Serpent (256 bit) dan kemudian dengan AES (256 bit).
d. AES-Twofish-Serpant, Tiga *cipher* beroperasi dalam mode XTS, dengan setiap *cipher* memiliki kunci independen. Setiap blok 128 bit pertama dienkripsi dengan Serpent (256 bit), kemudian dengan Twofish (256 bit), terakhir dengan AES (256 bit).

Kompleksitas algoritma menyatakan tingkat kerumitan dari cara kerja tiap algoritma. Kompleksitas algoritma berperan penting dalam sistem keamanan algoritma tersebut, semakin kompleks suatu algoritma, maka akan semakin sulit dan lama untuk dapat didekripsi oleh kriptanalis

III. RESEARCH METHOD

Metode penelitian yang dilakukan adalah dengan melakukan analisis pengguanaan aplikasi DiskCryptor. Akan dilakukan analisis mode operasi *blok cipher* yang diterapkan, kemudian akan dilakukan analisis panjang kunci yang digunakan oleh DiskCryptor, lalu untuk mengetahui apakah DiskCryptor memberikan fungsi pengamanan terhadap konten atau data yang ada di dalam media penyimpanan akan dilakukan uji forensik, terakhir akan dilakukan analisis waktu enkripsi dan dekripsi pada media penyimpanan dengan penggunaan algoritma dan ukuran kapasitas yang beragam.

IV. RESULTS AND DISCUSSION

A. *Penggunaan Mode Operasi*

Pada FDE terdapat tigabesar mode operasi *block cipher yaitu: electronic code book* (ECB), *cipher block chaining* (CBC), dan *counter* (CTR). Pada mode operasi ECB proses enkripsi dan dekripsi relatif cepat dan sederhana, namun ECB sangat tidak aman dalam mengenkripsi *disk* karena blok *plaintext* yang sama selalu menghasilkan *ciphertext* yang sama. Penyerang juga dapat melakukan *cut* dan *paste* pada blok dan sektor. Mode operasi CBC popular digunakan pada beberapa perangkat lunak FDE, seperti pada BitLocker. Penggunaan CBC memiliki kelemahan yaitu jika *initialization vector* (IV) dapat diprediksi oleh penyerang maka penyerang dapat menyimpan *file* atau kombinasi *file* yang dapat diidentifikasi bahkan setelah proses enkripsi atau dikenal dengan serangan *watermaking*. Selanjutnya mode operasi CTR merupakan mode operasi *block cipher* yang mampu diadaptasi menjadi *stream cipher*, CTR mempunyai kelemahan yang sama dengan CBC berkaitan dengan IV, pada CTR disebut *nonces*. Mode operasi yang banyak digunakan pada FDE saat ini dan menjadi standar untuk enkripsi *hard disk* adalah mode operasi *ciphertext stealing* (XTS). Berikut tabel penggunaan mode operasi dari beberapa aplikasi FDE.

TABLE II
PERBEDAAN PENGGUNAAN MODE OPERASI PADA FDE

Aplikasi	CBC dengan predictable IV	CBC dengan secret IV	CBC dengan kunci random per-sector	XTS
BestCrypt	-	√	-	√
BitLocker	-	√	-	√ (Windows 10)
CrossCrypt	√	-	-	-
DiskCryptor	-	-	-	√
TrueCrypt	√ (TrueCrypt versi 1.0 – 4.0)	-	-	√ (dari TrueCrypt versi 5.0)
Symantec	-	-	√	-
VeraCrypt	-	-	-	√

Asal mula mode XTS adalah mode XEX (XOR – Encrypt – XOR) yang dicipakan oleh Phillip Rogaway [5]. Menggunakan konstruksi Liskov, Rivest dan Wagner [6] yang mampu mengatasi kerentanan mode LRW. Pada tahun 2007 XEX distandarisasi oleh IEEE *(Institute of Electrical and Electronics Engineers, Inc.)* dengan modifikasi dan ekstensi. Pada bulan Januari 2010, mode XTS-AES disetujui oleh NIST sebagai mode operasi *block cipher* [7].

B. Panjang Kunci

Pada fungsi kriptografi, panjang kunci adalah parameter keamanan yang penting. NIST memberikan rekomendasi tentang algoritma kriptografi yang aman digunakan dalam rentang waktu dimana kunci tertentu diizinkan untuk digunakan atau kunci yang digunakan pada waktu tertentu masih akan tetap berlaku. Berikut Tabel III yang menunjukkan data tentang rekomendasi standarisasi penggunaan algoritma kriptografi NIST tahun 2016 [8].

TABLE III
REKOMENDASI NIST 2016

Rentang Waktu	Level Keamanan Minimum (bit)	Algoritma Simetris
2010 (Legacy)	80	3DES with 2 keys
2016 – 2030	112	3DES with 3 keys
2016 – 2030 dan seterusnya	128	AES-128
2016 – 2030 dan seterusnya	192	AES-192
2016 – 2030 dan seterusnya	256	AES-256

DiskCryptor menggunakan panjang kunci 256 bit untuk seluruh sandi algoritma maka sampai saat ini masih dianggap aman untuk digunakan hingga tahun 2030 dan seterusnya. Penggunaan kunci yang besar (256 bit) memberikan keamanan lebih terhadap serangan *brute force*, karena penyerang membutuhkan ruang kunci sebesar 2^{256} yang merupakan nilai yang sangat besar untuk melakukan komputasinya.

C. Data Forensik

Analisis data forensik dilakukan untuk mengetahui apakah DiskCryptor benar-benar memberikan fungsi pengamanan terhadap konten/data yang ada di dalam media penyimpanan. Oleh karena itu dilakukan analisa forensik untuk melihat apakah konten/data yang ada di dalam media penyimpanan yang telah terenkripsi benar-benar dalam bentuk yang tidak dapat dimengerti oleh pemilik media penyimpanan yang sah. Forensik yang dilakukan menggunakan bantuan *tools* Access Data FTK Imager dan Hex Workshop Hex Editor dengan membandingkan konten/data yang ada di dalam media penyimpanan terenkripsi dengan yang tidak tereknkripsi. Berikut isi *file* yang akan disimpan pada kedua media penyimpanan.

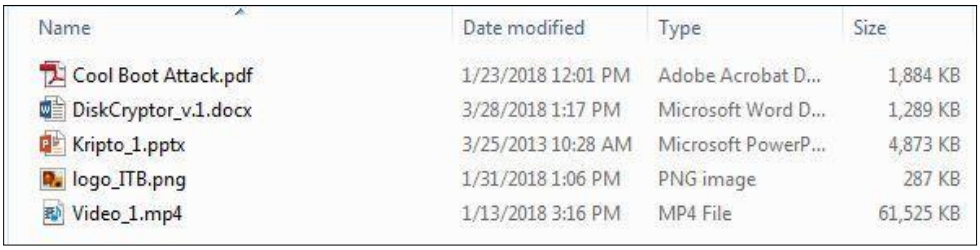
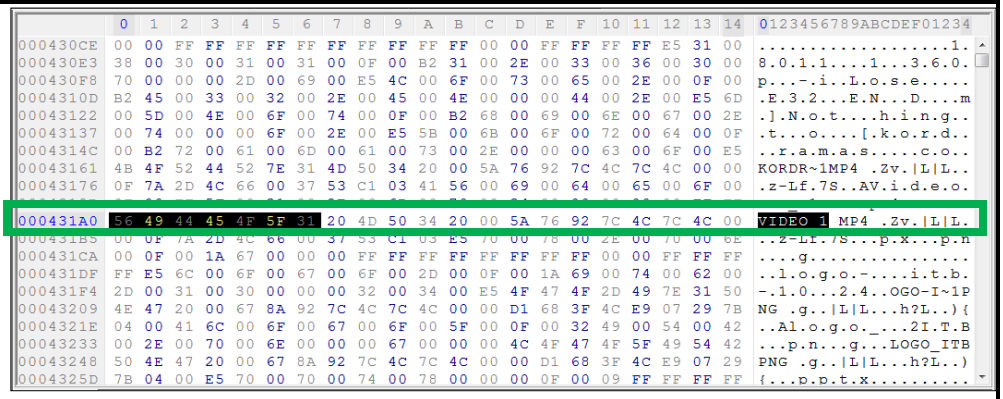
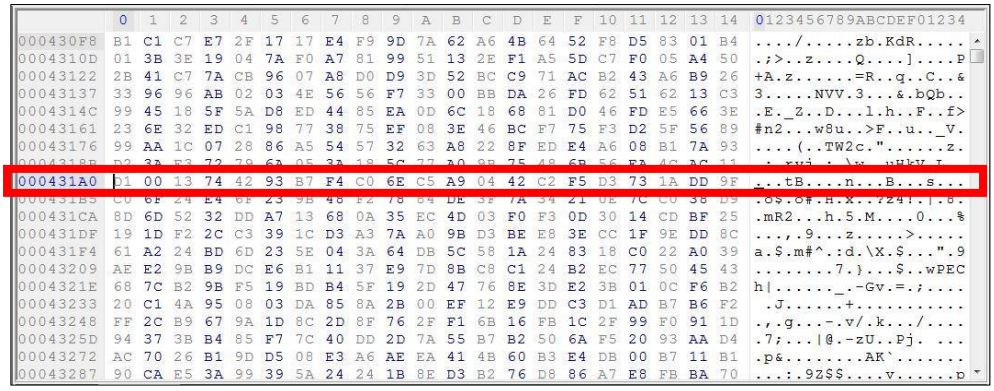


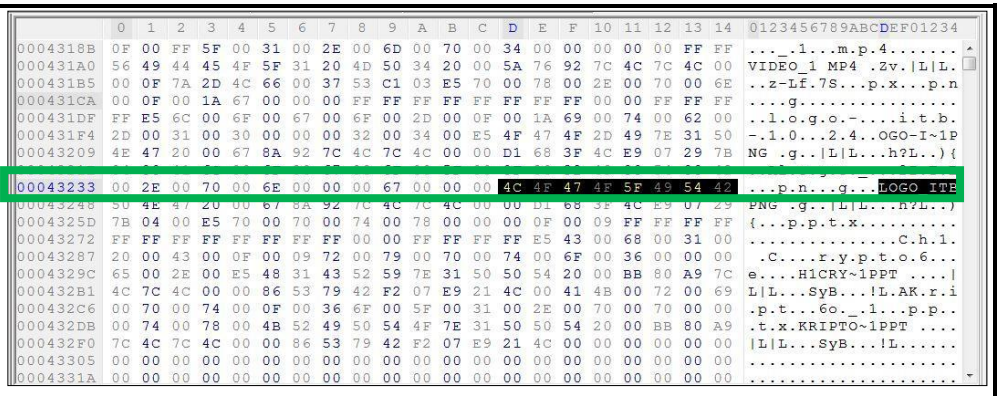
Fig. 1. Data yang Tersimpan pada Media Penyimpanan

Kemudian kedua media penyimpanan tersebut dibuat *file image* nya. Dengan Hex Workshop Hex Editor kedua *file image* akan dibandingkan dengan cara melakukan pencarian berdasarkan *string* nama data *file* yang tersimpan pada kedua *file image* tersebut, tujuannya untuk mengetahui apakah ada perbedaan dari keduanya. Adapun hasil yang didapat dari analisis data forensik adalah sebagai berikut:

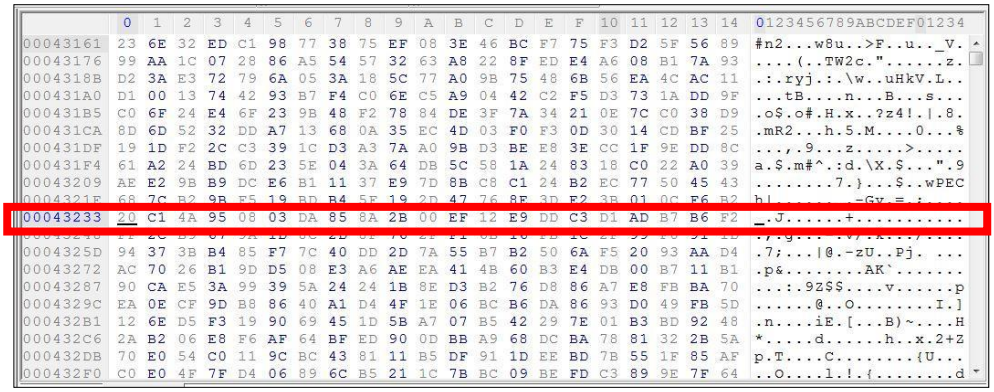
TABLE IV
TABEL PERBANDINGAN HASIL ANALISIS DATA FORENSIK

	HASIL
1	 *File image Video_1 sebelum dienkripsi*  *File image Video_1 setelah dienkripsi*

2



File image logo_ITB sebelum dienkripsi



File image logo_ITB setelah dienkripsi

Tabel IVdi atas menunjukan hasil pencarian nama *file* untuk *file* Video_1.MP4 dan *file* logo_ITB.png dapat diketahui bahwa pada media penyimpanan yang tidak terenkripsi *file* tersebut masih dapat ditemukan pada *data offset* 0x000431A0 untuk *file* Video_1.MP4 dan 0x00043233 untuk *file* logo_ITB.png. Sedangkan ketika melakukan pencarian berdasarkan *string* nama *file* yang sama pada *file image* media penyimpanan yang terenkripsi. Didapat hasil sebagai berikut:

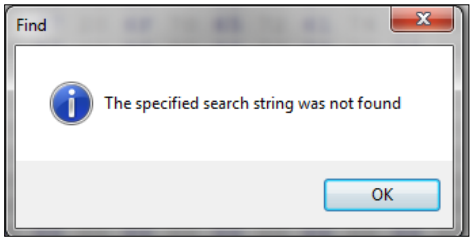


Fig. 2. Hasil Pencarian File Berdasarkan String pada File *Image* terenkripsi

Karena hasil pencarian berdasarkan *string* dari nama *file* tidak berhasil dilakukan, untuk meyakinkan bahwa data pada media penyimpanan benar-benar terenkripsi dilakukan pencarian dengan berdasarkan *data offset* dari *file* yang akan dicari. Untuk *file* Video_1.MP4 diketahui *data offset* nya adalah 0x 000431A0 dan untuk *file* logo_ITB.png di *data offset* 0x00043233.

Kesimpulan yang didapat adalah bahwa DiskCryptor benar-benar melakukan fungsinya sebagai perangkat lunak enkripsi yang mampu menjaga kerahasiaan data yang tersimpan pada media penyimpanan. Pada hasil pencarian pada *file image* yang terenkripsi dapat diketahui *file* tidak dapat ditemukan dan seluruh kapasitas atau data pada media penyimpanan diubah menjadi bentuk yang hanya bisa dimengerti oleh orang yang memiliki kunci untuk mendeskripsi data yang telah dienkripsi.

D. Analisis Waktu Enkripsi dan Dekripsi

Waktu adalah salah satu faktor dalam melakukan proses enkripsi dan dekripsi. Dengan mengetahui waktu yang diperlukan, kecepatan proses enkripsi dan dekripsi dapat diketahui. DiskCryptor mendukung 7 macam algoritma yang dapat diterapkan dalam mode XTS. Untuk mengetahui kecepatan proses enkripsi dan dekripsi dari tiap algoritma maka dilakukan pengujian terhadap satu buah flashdisk USB 2.0 dengan kapasitas 2GB. Pengujian dilakukan pada laptop dengan prosesor Intel Core i3-3110M CPU @ 2.4 GHz. Dari pengujian didapat hasil sebagai berikut:

TABLE IV
HUBUNGAN ANTARA JENIS ALGORITMA DENGAN WAKTU PROSES ENKRIPSI DAN PROSES DEKRIPSI

Algoritma	Waktu	
	Enkripsi	Dekripsi
AES	3 menit 59 detik	3 menit 51 detik
Twofish	3 menit 53 detik	3 menit 52 detik
Serpent	3 menit 50 detik	3 menit 47 detik
AES-Twofish	4 menit 8 detik	4 menit 7 detik
Twofish-Serpent	4 menit 7 detik	4 menit 5 detik
Serpent-AES	4 menit 5 detik	4 menit 4 detik
AES-Twofish-Serpent	4 menit 19 detik	4 menit 16 detik

Dari hasil yang didapat tidak terjadi perbedaan yang signifikan dari semua jenis algoritma yang diterapkan untuk proses enkripsi maupun proses dekripsi. Algoritma Serpent memerlukan waktu yang paling cepat diantara ketujuh algoritma yang diuji. Hasil ini sesuai dengan pengujian yang dilakukan pada [4] bahwa optimalisasi penggunaan algortima tergantung dari jenis prosesor yang digunakan, dalam hal ini prosesor Intel Core i3 optimal menggunakan algoritma Serpent. Dari data tersebut akan dilakukan pengujian lebih lanjut untuk mengetahui hubungan antara algoritma Serpent terhadap kapasitas flashdisk yang berbeda-beda. Keempat flashdisk yang digunakan merupakan flashdisk USB 2.0. Adapun spesifikasi empat flashdisk yang digunakan adalah sebagai berikut:

a. Toshiba Transmemory 2GB
b. Kingston DT101G2 4GB
c. Toshiba Transmemory 8GB
d. HP 16 GB

TABLE V
HUBUNGAN ANTARA UKURAN VOLUME DENGAN WAKTU PROSES ENKRIPSI DAN PROSES DEKRIPSI

Ukuran	Type File System	Estimasi Waktu	
		Enkripsi	Dekripsi
Toshiba 2GB	FAT32	3 menit 50 detik	3 menit 47 detik
Kingston 4GB	FAT32	23 menit 21 detik	23 menit 12 detik
Toshiba 8GB	FAT32	31 menit 3 detik	24 menit 57 detik
HP 16 GB	FAT32	1 jam 6 menit	49 menit 39 detik

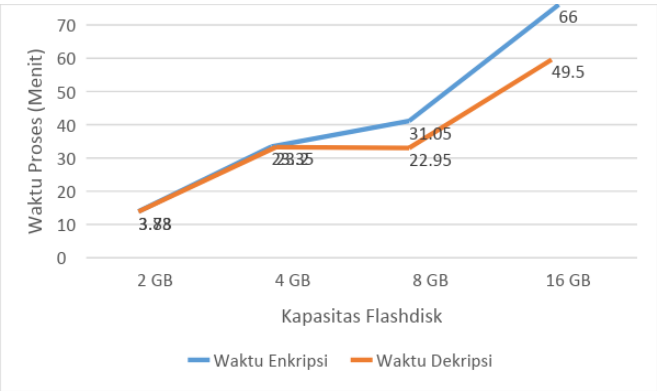


Fig. 3. Grafik Hubungan antara Ukuran Volume dengan Waktu Proses Enkripsi dan Proses Dekripsi

Pada Fig 3 menunjukan kecenderungan kenaikan waktu yang dibutuhkan untuk melakukan proses enkripsi dan dekripsi. Semakin besar ukuran atau kapasitas media penyimpanan maka semakin lama pula waktu yang dibutuhkan untuk melakukan proses enkripsi dan proses dekripsi. Dilihat dari tabel IV dan V proses dekripsi yang dilakukan aplikasi DiskCryptor memerlukan waktu yang lebih cepat jika dibandingkan dengan proses enkripsinya.

V. Conclusion

Aplikasi DiskCryptor merupakan aplikasi enkripsi yang dapat diterapkan untuk *volume* (VE) dan *full disk* (FDE). Pemilihan algoritma enkripsi dan fungsi pembangkitan bilangan acak pada aplikasi DiskCryptor dapat dikatakan memenuhi kriteria aspek kriptografi terkini. Penggunaan aplikasi DiskCryptor memberikan layanan jaminan keamanan data/konten yang ada di dalam media penyimpanan digital, baik dalam bentuk *volume* disk ataupun full disk. Namun tidak menutup adanya ancaman terhadap keamanan aplikasi DiskCryptor. Oleh karena itu, Aplikasi Diskcryptor dapat menjadi solusi yang baik untuk enkripsi media penyimpanan (*VE* atau *FDE*). Untuk pengembangan selanjutnya dapat dilakukan analisis celah keamanan *(side channel)* atau serangan-serangan yang mungkin terjadi pada aplikasi DiskCryptor.

REFERENCES

[1] Bill Clinten, "Hard Disk Berisi Data Gaji Karyawan Facebook Dicuri," Des 16, 2019. https://tekno.kompas.com/read/2019/12/16/09121837/hard-disk-berisi-data-gaji-karyawan-facebook-dicur
[2] U.S. Departement of Health and Human Services, "Breach Portal: Notice to the Secretary of HHS Breach of Unsecured Protected Health Information," 2017.
[3] R. Olsson, "Performance differences in encryption software versus storage devices," Student thesis, 2012. Diakses: Jun 20, 2012. [Daring]. Tersedia pada: http://urn.kb.se/resolve?urn=urn:nbn:se:lnu:diva-20315
[4] Ntldr, "DiskCryptor," Des 14, 2015. https://diskcryptor.org/
[5] P. Rogaway, "Efficient Instantiations of Tweakable Blockciphers and Refinements to Modes OCB and PMAC," dalam *Advances in Cryptology - ASIACRYPT 2004*, vol. 3329, P. J. Lee, Ed. Berlin, Heidelberg: Springer Berlin Heidelberg, 2004, hlm. 16–31. doi: 10.1007/978-3-540-30539-2_2.
[6] M. Liskov, R. L. Rivest, dan D. Wagner, "Tweakable Block Ciphers," *Journal of Cryptology*, vol. 24, no. 3, hlm. 588–613, Jul 2011, doi: 10.1007/s00145-010-9073-y.
[7] M. Dworkin, "Recommendation for block cipher modes of operation: the XTS-AES mode for confidentiality on storage devices," *COMPUTER SECURITY*, hlm. 12.
[8] BlueCrypt, "National Institute of Standards and Technology (NIST). Key Recomendation keylength," Feb 28, 2018.